J. Aust. Math. Soc. **91** (2011), 103–124
doi:10.1017/S1446788711001443

A SIMPLE GEOMETRIC CONSTRUCTION INVOLVING ULTRARADICALS

J. ROBERTSON and C. SNYDER✉

(Received 25 August 2010; accepted 15 May 2011)

Communicated by M. G. Cowling

In memory of Curt Meyer (19 November 1919–18 April 2011)

Abstract

We give a new type of geometric construction that allows for the construction of families of quintic irrationalities, and is quite rich in algebraic properties. This construction may be considered as our first attempt at characterizing points constructible with compass and twice-notched ruler, a problem that seems to have been known in some form for more than two millennia.

2010 *Mathematics subject classification*: primary 51M15.
Keywords and phrases: constructible number, marked-ruler construction, quintic extension, ultraradical.

1. Introduction

Geometric constructions have been a source of fascination since antiquity. Euclid gave interesting and nontrivial constructions using only the familiar tools of a straightedge and compass. The ancient Greeks must have been sure that certain constructions were impossible, such as trisecting a given angle or duplicating a cube; however, a complete characterization of constructible points in a coordinate plane had to wait until more modern times, after analytic geometry and algebra, in particular field theory, had been invented and well established.

On the other hand, the ancient Greeks were not afraid of extending the assortment of tools they used so as to create more types of constructions. For example, one way uses intersections of conics, which allowed for trisection of angles. Another method uses a marked ruler instead of a straightedge. A characterization of the constructible points is known in some instances but not in others, depending on the tools used. See below for more details.

Here is some motivation for the work presented here. Suppose that we can use a twice-notched ruler (or marked ruler for short), that is, a straightedge with two

marks one unit apart, and a compass. See [1, 4] for a description of this type of construction. If we start with the points $(0, 0)$ and $(1, 0)$, then it is an open problem to give an algebraic characterization of the points that can be constructed by these tools. For example, it is not known if there is a way to construct the real $\sqrt[5]{2}$ or to quinsect a given angle, even though there are numbers satisfying irreducible quintic polynomials over $\mathbb{Q}$ constructible using only these tools. In this note we give a new type of construction that has a rich set of constructible points, including many whose coordinates are roots of quintic polynomials, but for which an algebraic characterization of the constructible points is much more manageable than for a twice-notched ruler and compass. We do not know if our modified construction process is subsumed under that of the twice-notched ruler and compass, but we would guess that it is. In any case, perhaps surprisingly, all real fifth roots of rational numbers (among many others) are constructible by our modified method.

2. Tools for q-constructions

Here, we set up our construction, and define constructible points and numbers.

We shall be working in $\mathbb{R} \times \mathbb{R}$. We call a point in $\mathbb{R} \times \mathbb{R}$ *q-constructible* if it is the last point in a finite sequence of points $P_1, P_2, \ldots, P_n$ such that the point is in the 'starter' set

$$\{(0, 0), (1, 0), (0, 1)\},$$

or is obtained inductively in one of the following ways:

(i) as the intersection of two lines, each of which passes through two points that appear earlier in the sequence;
(ii) as an intersection of a line passing through two earlier points and a circle passing through $(0, 0)$ and centered at a point on the x-axis appearing earlier in the sequence;
(iii) as a point of intersection of the graph of $y = x^3$ and a line described in (i);
(iv) as a point of intersection of the graph of $y = x^3$ and a circle described in (ii).

A real number will be called *q-constructible*, if it is the x-coordinate of a q-constructible point lying on the x-axis. A line passing through two q-constructible points will be called a *q-constructible line*. Also, for convenience, we call the sequence of points $P_1, \ldots, P_n$ in the definition a *q-constructible sequence*.

Here are some reasons for looking at this particular type of construction. First of all, if we use the conic $y = x^2$ instead of our cubic $y = x^3$ along with a straightedge and compass, then the set of points that are constructible is the same as the set of points obtained by using only a marked ruler. See [1, 4, 8] for more details. The numbers constructible by this process are precisely those that lie in a real 2–3-tower over $\mathbb{Q}$. This means that a is constructible by this process if and only if there exists a sequence of field extensions $K_0, K_1, \ldots, K_n$ such that

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R},$$

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

where $[K_j : K_{j-1}] = 2$ or 3, for $j = 1, \ldots, n$, and $a \in K_n$. Notice in particular that intersecting two conics yields at most four points by Bezout's theorem. Hence the numbers constructed this way satisfy polynomials of degree at most four over fields generated by previously constructed numbers. Thus, by the solutions of cubic and quartic equations by Cardano and Ferrari, it is easily seen that the numbers do indeed lie in real 2–3-towers over $\mathbb{Q}$.

Next, if we allow a marked ruler and compass, then it is not too hard to show that the numbers constructible by this process satisfy equations of degree at most six. See [1] for a very nice presentation of this fact and others. Hence by replacing the marked ruler with the cubic $y = x^3$, we would expect solutions to equations of degree at most six. See [8] for other suggestions of cubics. However, by our restriction on the use of the compass, we shall see that the degree is at most five; hence the 'q' in q-construction stands for 'quintic'.

One of our results gives an algebraic characterization of q-constructible numbers.

A real number a is q-constructible if and only if there exists a sequence of field extensions $K_0, K_1, \ldots, K_n$ with $a \in K_n$ such that

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R},$$

where $[K_j : K_{j-1}] \in \{1\ 2, 3\ 5\}$, for all $j = 1, \ldots, n$, and if $[K_j : K_{j-1}] = 5$ then $K_j = K_{j-1}(\sqrt[5]{a_{j-1}})$ where $a_{j-1} \in K_{j-1}$ is the unique real root of the polynomial $x^5 + x - a_{j-1}$.

3. A characterization of q-constructible numbers

As promised, we give a characterization of q-constructible numbers. However, we first introduce some notation and terminology for convenience.

We denote by $\mathbb{F}$ the set of all q-constructible numbers.

If a is a real number, then the unique real root of the polynomial $x^5 + x - a$ is called the *ultraradical* of a and is denoted by $\sqrt[5]{a}$. If $a \in F$, where F is a subfield of $\mathbb{R}$, then $F(\sqrt[5]{a})$ will be called an *ultraradical extension* of F.

Let $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}$ be a tower of field extensions, with $[K_j : K_{j-1}] = 1$, 2, 3, or 5 (where $j = 1\ 2, \ldots, n$), such that K_j is an ultraradical extension of K_{j-1} if the degree is five. We shall call such an extension a *(real) q-tower* of $\mathbb{Q}$.

Given this notation, here is a statement of one of our results.

THEOREM 1. *A real number a lies in $\mathbb{F}$ if and only if $a \in K_n$ for some real q-tower $K_0 \subseteq \cdots \subseteq K_n$ of $\mathbb{Q}$.*

The proof will be carried out in several steps.

PROPOSITION 2. *Let $P_j = (a_j, b_j)$, for $j = 1, \ldots, m$, be a q-constructible sequence of points. Then there is a real q-tower $K_0, \ldots, K_n$ of $\mathbb{Q}$ such that $a_j, b_j \in K_n$ for all j.*

PROOF. We use induction on m. For $m = 1$, $P_1 = (a_1, b_1) \in \{(0, 0), (1, 0), (0, 1)\}$ and thus $a_1, b_1 \in \mathbb{Q} = K_0$.

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

Now assume that $m > 1$ and that the proposition holds for any q-constructible sequence of less than m points. Let $P_1, \ldots, P_m$ be a q-constructible sequence of m points. Hence by the induction hypothesis there is a real q-tower $K_0, \ldots, K_n$ such that $a_j, b_j \in K_n$ for all $j < m$. Now consider $P_m = (a_m, b_m)$. Then P_m is a point of intersection of curves in four possible ways, which we now consider individually.

Suppose that P_m is the intersection of two lines, each passing through two earlier points in the sequence. Then the lines have equations with coefficients in K_n, and thus the coordinates of the point of intersection are in K_n.

Next suppose that P_m is a point of intersection of a line passing through two earlier points in the sequence and a circle passing through $(0, 0)$ and centered at a point on the x-axis appearing earlier in the sequence. Then the line and circle have equations with coefficients in K_n, and so $a_m, b_m \in K_n(\sqrt{c})$ for some $c \in K_n$ with $c > 0$. Hence $a_m, b_m \in K_{n+1} = K_n(\sqrt{c})$, and $[K_{n+1} : K_n] = 1$ or 2, and $K_{n+1} \subseteq \mathbb{R}$. Thus $a_m, b_m \in K_{n+1}$, the terminal field of a real q-tower of $\mathbb{Q}$.

Now suppose that P_m is a point of intersection of the curve $y = x^3$ and a line passing through two points appearing earlier in the sequence. As above, the line has an equation with coefficients in K_n. Thus a_m is a real root of a cubic polynomial with coefficients in K_n. Let $K_{n+1} = K_n(a_m)$. Then $K_{n+1} \subseteq \mathbb{R}$ and $[K_{n+1} : K_n] \leq 3$. Moreover $b_m \in K_{n+1}$, since $b_m = a_m^3$.

Finally, suppose that P_m is a point of intersection of the curve $y = x^3$ and the circle passing through $(0, 0)$ and with center $P_j = (a_j, 0)$ for some $j < m$. Hence $a_j \in K_n$. The circle has an equation $y^2 + x^2 - 2a_j x = 0$. Thus a_m must satisfy the sextic equation $x^6 + x^2 - 2a_j x = 0$. If $a_m = 0$, then $P_m = (0, 0)$ and we are done. If not, then a_m satisfies the quintic equation

$$x^5 + x - a = 0,$$

where $a = 2a_j \in K_n$. Hence $a_m = \sqrt[5]{a}$. So if we let $K_{n+1} = K_n(\sqrt[5]{a})$, then $[K_{n+1} : K_n] \leq 5$. We shall be done if we can show $[K_{n+1} : K_n] \neq 4$. Assume otherwise, then

$$x^5 + x - a = p(x)q(x),$$

where p and q are irreducible polynomials over K_n of degrees four and one respectively. By assumption, $\sqrt[5]{a}$ is a root of p. However, q also has a real root, implying $\sqrt[5]{a}$ must be this root, since the real root of $x^5 + x - a$ is unique. This is the desired contradiction, and the proposition is now established. □

From this proposition, we immediately obtain the following result.

Corollary 3. *If $a \in \mathbb{F}$, then $a \in K_n$ for some real q-tower $K_0, \ldots, K_n$ of $\mathbb{Q}$.*

Now we consider the converse. However, we first isolate a useful lemma that follows essentially by observing that one can prove $\mathbb{F}$ is a field by using only a straightedge.

Lemma 4. *The set $\mathbb{F}$ is a subfield of $\mathbb{R}$.*

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

Proof. We just sketch the argument. First note that the points $(1, 0)$, $(0, 1)$, $(2, 0)$ and $(0, 2)$ are q-constructible, for the first two are in our starter set; $(2, 0)$ and $(1, 1)$ are intersections of the (q-constructible) x-axis and the curve $y = x^3$ respectively with the circle through $(0, 0)$ centered at $(1, 0)$. However, $(0, 2)$ is then the intersection of the q-constructible lines $x + y = 2$ and the y-axis. This new starter set is all that is necessary to show that the numbers constructible from this set by using only a straightedge form a field; see [4, Ch. 4].

We now take advantage of Martin's presentation. In [4, Ch. 4], starting with Theorem 4.4 through Corollary 4.11, replace the words 'ruler point' and 'ruler line' with 'q-constructible point' and 'q-constructible line' respectively. The proofs of all the results remain unchanged and the new Corollaries 4.9 and 4.11 show that $\mathbb{F}$ is a field. For later use, we note that by the new Theorem 4.7, any line through a q-constructible point and parallel to a q-constructible line is a q-constructible line. □

For a detailed proof of this lemma, see [6].

We now use this lemma and its proof to help prove the converse to Corollary 3.

Proposition 5. *Let $K_0, \ldots, K_n$ be a real q-tower of $\mathbb{Q}$. Then $K_n \subseteq \mathbb{F}$.*

Proof. We proceed by induction on n. If $n = 0$, then $K_n = \mathbb{Q} \subseteq \mathbb{F}$, since $\mathbb{F}$ is a field.

Now suppose that $n > 1$ and that all q-towers of $\mathbb{Q}$ of length less than n are contained in $\mathbb{F}$. Let $K_0, \ldots, K_n$ be a real q-tower of $\mathbb{Q}$. Then by the induction hypothesis, $K_{n-1} \subseteq \mathbb{F}$. We consider three cases depending on the degree $[K_n : K_{n-1}]$.

First, suppose that $[K_n : K_{n-1}] = 2$. Then $K_n = K_{n-1}(\sqrt{a})$ for some $a \in K_{n-1}$ with $a > 0$. We claim that $\sqrt{a}$ is q-constructible. The argument is essentially the same as for the Poncelet–Steiner theorem, which shows (roughly) that points constructible by straightedge and one circle are precisely those constructible by the usual straightedge and compass; see [4, Ch. 6]. Thus square roots can be constructed.

Notice that $a > 0$, and so $-1 < (a - 1)/(a + 1) < 1$ and $0 < (a - 1)/(a + 1) + 1 < 2$. Since $a \in \mathbb{F}$ by the induction hypothesis, $(a - 1)/(a + 1) + 1 \in \mathbb{F}$, as $\mathbb{F}$ is a field. By the last statement in the proof of the lemma, the vertical line through the point $((a - 1)/(a + 1) + 1, 0)$ is q-constructible. Hence the points

$$\left(\frac{a-1}{a+1} + 1, \pm\sqrt{1 - \left(\frac{a-1}{a+1}\right)^2}\right)$$

of intersection of this line with the circle passing through $(0, 0)$ centered at $(1, 0)$ (thus with an equation $y^2 + (x - 1)^2 = 1$) are q-constructible. However, by the last statement of the proof of the lemma again, by projecting to the y-axis and then along a line of slope -1 we then see that

$$\sqrt{1 - \left(\frac{a-1}{a+1}\right)^2} \in \mathbb{F}.$$

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

However, we now have

$$\sqrt{a} = \left(\frac{a+1}{2}\right)\sqrt{1 - \left(\frac{a-1}{a+1}\right)^2} \in \mathbb{F},$$

as desired.

Next suppose that $[K_n : K_{n-1}] = 3$. Then $K_n = K_{n-1}(\alpha)$, where α is the real root of an irreducible cubic polynomial p over K_{n-1}. We claim that $\mathbb{F}$ is Vietian; that is, if $a \in \mathbb{F}$ with $a > 0$, then $\sqrt{a}, \sqrt[3]{a} \in \mathbb{F}$, and, moreover, if $\cos\theta \in \mathbb{F}$, then $\cos(\theta/3) \in \mathbb{F}$. To see this, suppose that $a \in \mathbb{F}$ with $a > 0$; notice from the previous argument that $\sqrt{a} \in \mathbb{F}$. Moreover, $(\sqrt[3]{a}, a)$ is the intersection of the q-constructible line $y = a$ with $y = x^3$ and thus q-constructible. Projecting to the x-axis shows $\sqrt[3]{a} \in \mathbb{F}$. Finally, let $a = 2\cos\theta \in \mathbb{F}$. Then $x = 2\cos(\theta/3)$ satisfies the equation $x^3 - 3x - a = 0$. However, this is the x-coordinate of the intersection of the line $y = 3x + a$, which is q-constructible, and the curve $y = x^3$. Thus $2\cos(\theta/3)$ and hence also $\cos(\theta/3)$ are in $\mathbb{F}$. Therefore, $\mathbb{F}$ is Vietian as claimed. However, by [4, Theorem 9.8], which states that a real root of any polynomial of degree less than five over a Vietian field lies in this field, we then have $\alpha \in \mathbb{F}$. Therefore, since $\mathbb{F}$ is again a field, $K_n \subseteq \mathbb{F}$.

Finally, suppose that $[K_n : K_{n-1}] = 5$. Then $K_n = K_{n-1}(\alpha)$ where $\alpha = \sqrt[5]{a}$ for some $a \in K_{n-1} \subseteq \mathbb{F}$; that is, α is the unique real root of $x^5 + x - a$. However, the points of intersection of $y = x^3$ with the circle passing through $(0, 0)$ centered at $(a/2\ 0)$ are then q-constructible. These points are easily seen to be $(0, 0)$ and (α, α^3). By projection, $\alpha \in \mathbb{F}$. Therefore $K_n \subseteq \mathbb{F}$, as desired.

This establishes the proposition. □

Corollary 3 and Proposition 5 establish the theorem, that is, an algebraic characterization of the q-constructible numbers.

4. More properties and some examples of q-constructible numbers

We saw in the proof of Proposition 5 that the field $\mathbb{F}$ of q-constructible numbers is Vietian, and so any real root of a polynomial over $\mathbb{F}$ of degree at most four is also q-constructible. Now we address the problem of the q-constructibility of real roots of quintic polynomials over $\mathbb{F}$. First we show that $\mathbb{F}$ is closed under taking fifth roots.

THEOREM 6. *If $r \in \mathbb{F}$, then the real fifth root $\sqrt[5]{r} \in \mathbb{F}$.*

Hence, as noted in the introduction, all fifth roots of rational numbers are q-constructible.

Note that it suffices to prove the theorem for positive r. Moreover, we need only prove the theorem when $r \geq 2$ (or r is sufficiently large), since we can reduce the problem to this case by multiplying by a fifth power of a sufficiently large integer.

We prove the theorem in several steps. In what follows, if $r \in \mathbb{R}$, then $\sqrt[5]{r}$ always means the real fifth root.

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

Proposition 7. *Suppose that K is a subfield of $\mathbb{R}$ and a finite extension of $\mathbb{Q}$. Suppose, too, that $r \in K$, $r \geq 2$ and the polynomial $x^5 - r$ is irreducible in $K[x]$. Then there exists an extension L in $\mathbb{R}$ of K of degree at most three, and there are numbers $a, b \in L$ with $a > 0$, such that if β is the real root of the polynomial $x^5 + ax + b$, then $L(\sqrt[5]{r}) = L(\beta)$.*

Proof. Let $\alpha = \sqrt[5]{r}$. Then $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ is a basis of $L(\alpha)/L$ (where L will be determined below). Let $\beta = a_0 + a_1\alpha + \cdots + a_4\alpha^4$ for some $a_j \in L$. We shall determine the root β described in the statement of the proposition. Since $x^5 - r = \prod_{j=1}^{5}(x - \alpha\zeta^j)$, where $\zeta = \zeta_5$ is a primitive fifth root of unity in $\mathbb{C}$, the minimal polynomial p of β over L is given as $p(x) = \prod_{j=1}^{5}(x - \beta_j)$, where $\beta_j = \sum_{\mu=0}^{4} a_\mu \zeta^{j\mu}\alpha^\mu$. Also,

$$p(x) = x^5 - \sigma_1 x^4 + \sigma_2 x^3 - \sigma_3 x^2 + \sigma_4 x - \sigma_5,$$

where the σ_j are the elementary symmetric functions of $\beta_1, \ldots, \beta_5$, that is,

$$\sigma_j(x_1, \ldots, x_5) = \sum_{1 \leq k_1 < \cdots < k_j \leq 5} x_{k_1} \cdots x_{k_j}$$

for $j = 1, \ldots, 5$, where $x_k = \beta_k$.

Since $p(x) = x^5 + ax + b$, we want $\sigma_1 = \sigma_2 = \sigma_3 = 0$. Instead of working directly with the σ, it is easier to use the following power sums of the roots. Let

$$s_j = s_j(\beta_1, \ldots, \beta_5) = \sum_{k=1}^{5} \beta_k^j.$$

Relations between the elementary symmetric functions and the power sums are given by Newton's identities, see [3]:

$$s_j - \sigma_1 s_{j-1} + - \cdots + (-1)^{j-1}\sigma_{j-1}s_1 + (-1)^j j\sigma_j = 0,$$

for $j = 1, \ldots, 5$.

Notice that $\sigma_1 = \sigma_2 = \sigma_3 = 0$ if and only if $s_1 = s_2 = s_3 = 0$. Given the latter, we derive relations among $a_0, \ldots, a_4$ defined above.

We start with

$$s_1 = 0.$$

Notice then that

$$s_1 = \sum_{i=1}^{5} \beta_i = \sum_{i=1}^{5} \sum_{\mu=0}^{4} a_\mu \zeta^{i\mu}\alpha^\mu = \sum_{\mu=0}^{4} a_\mu \alpha^\mu \sum_{i=1}^{5} \zeta^{i\mu} = 5a_0,$$

since $\sum_{i=1}^{5} \zeta^{i\mu}$ is equal to 0 if $\mu \not\equiv 0 \bmod 5$, but is equal to 5 otherwise. Therefore,

$$a_0 = 0,$$

which we assume from now on.

Now we consider

$$s_2 = 0.$$

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

In this case,

$$\begin{aligned} s_2 &= \sum_{i=1}^{5} \beta_i^2 = \sum_{i=1}^{5} \Big(\sum_{\mu=1}^{4} a_\mu \zeta^{i\mu} \alpha^\mu \Big)^2 \\ &= \sum_{i=1}^{5} \Big(\sum_{\mu=1}^{4} a_\mu^2 \alpha^{2\mu} \zeta^{2\mu i} + 2 \sum_{1 \le \mu < \nu \le 4} a_\mu a_\nu \alpha^{\mu+\nu} \zeta^{(\mu+\nu)i} \Big) \\ &= \sum_{\mu=1}^{4} a_\mu^2 \alpha^{2\mu} \sum_{i=1}^{5} \zeta^{2\mu i} + 2 \sum_{1 \le \mu < \nu \le 4} a_\mu a_\nu \alpha^{\mu+\nu} \sum_{i=1}^{5} \zeta^{(\mu+\nu)i} \\ &= 5(2a_1 a_4 + 2a_2 a_3)\alpha^5 = 5(2a_1 a_4 + 2a_2 a_3) r, \end{aligned}$$

since $\sum_{i=1}^{5} \zeta^{2\mu i} = 0$ for $\mu = 1, \ldots, 4$ and $\sum_{i=1}^{5} \zeta^{(\mu+\nu)i} = 0$, unless $\mu + \nu$ is a multiple of 5. From this we obtain

$$a_1 a_4 + a_2 a_3 = 0.$$

Next we consider

$$s_3 = 0.$$

Here

$$\begin{aligned} s_3 &= \sum_{i=1}^{5} \beta_i^3 = \sum_{i=1}^{5} \Big(\sum_{\mu=1}^{4} a_\mu \zeta^{i\mu} \alpha^\mu \Big)^3 \\ &= \sum_{\mu=1}^{4} a_\mu^3 \alpha^{3\mu} \sum_{i=1}^{5} \zeta^{3\mu i} + 3 \sum_{\substack{1 \le \mu, \nu \le 4 \\ \mu \ne \nu}} a_\mu^2 a_\nu \alpha^{2\mu+\nu} \sum_{i=1}^{5} \zeta^{(2\mu+\nu)i} \\ &\quad + 6 \sum_{1 \le \mu < \nu < \varkappa \le 4} a_\mu a_\nu a_\varkappa \alpha^{\mu+\nu+\varkappa} \sum_{i=1}^{5} \zeta^{(\mu+\nu+\varkappa)i} \\ &= 15((a_1^2 a_3 + a_1 a_2^2)\alpha^5 + (a_3^2 a_4 + a_4^2 a_2)\alpha^{10}), \end{aligned}$$

since the first and third sums are zero and the second is nonzero only when $(\mu, \nu) \in \{(1, 3), (3, 4), (2, 1), (4, 2)\}$. Now using the fact that $\alpha^5 = r$ and the assumption that $s_3 = 0$, we obtain

$$a_1 a_2^2 + a_1^2 a_3 + (a_2 a_4^2 + a_3^2 a_4) r = 0.$$

Now we need to ensure that $a > 0$. Notice that $a = \sigma_4$, and by Newton's identity, with $s_1 = s_2 = s_3 = 0$, it follows that $s_4 + 4\sigma_4 = 0$ and thus

$$a = -\tfrac{1}{4} s_4.$$

We now compute s_4 in terms of the a_i. Notice that

$$s_4 = \sum_{i=1}^{5} \beta_i^4 = \sum_{i=1}^{5} \Big(\sum_{\mu=1}^{4} a_\mu \zeta^{i\mu} \alpha^\mu \Big)^4 = S_1 + S_2 + S_3 + S_4 + S_5,$$

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

where some calculation shows that

$$S_1 = \sum_{\mu=1}^{4} a_\mu^4 \alpha^{4\mu} \sum_{i=1}^{5} \zeta^{4\mu i} = 0,$$

$$S_2 = 4 \sum_{\mu\neq\nu} a_\mu^3 a_\nu \alpha^{3\mu+\nu} \sum_{i=1}^{5} \zeta^{(3\mu+\nu)i} = 20(a_1^3 a_2 r + (a_2^3 a_4 + a_1 a_3^3) r^2 + a_3 a_4^3 r^3),$$

$$S_3 = 6 \sum_{\mu<\nu} a_\mu^2 a_\nu^2 \alpha^{2(\mu+\nu)} \sum_{i=1}^{5} \zeta^{2(\mu+\nu)} = 30(a_1^2 a_4^2 + a_2^2 a_3^2) r^2,$$

$$S_4 = 12 \sum_{\substack{|\{\mu,\nu,\varkappa\}|=3 \\ \mu<\nu}} a_\mu^2 a_\nu a_\varkappa \alpha^{2\mu+\nu+\varkappa} \sum_{i=1}^{5} \zeta^{(2\mu+\nu+\varkappa)i} = 0,$$

and, finally,

$$S_5 = 24 a_1 a_2 a_3 a_4 \alpha^{10} \sum_{i=1}^{5} \zeta^{10i} = 120 a_1 a_2 a_3 a_4 r^2.$$

Therefore, $-4a = s_4$, and this is equal to

$$10r(2a_1^3 a_2 + r(2a_2^3 a_4 + 2a_1 a_3^3 + 3a_1^2 a_4^2 + 3a_2^2 a_3^2 + 12 a_1 a_2 a_3 a_4) + 2a_3 a_4^3 r^2).$$

Summarizing what we have so far,

$$\beta = a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4$$

is a root of $p(x) = x^5 + ax + b$, if the a_i satisfy the two conditions,

$$a_1 a_4 + a_2 a_3 = 0, \tag{1}$$

$$a_1 a_2^2 + a_1^2 a_3 + (a_2 a_4^2 + a_3^2 a_4) r = 0. \tag{2}$$

Now let $a_3 = -1$ and $a_4 = 1$; thus by (1), $a_1 = a_2$. Hence by (2),

$$a_1^3 - a_1^2 + (a_1 + 1) r = 0.$$

However, we then have

$$s_4 = 10r(2a_1^4 + (2a_1^3 - 6a_1^2 - 2a_1) r - 2r^2).$$

Therefore in order that $a > 0$, we need $s_4 < 0$ or, equivalently, that

$$c = r^2 + (a_1 + 3a_1^2 - a_1^3) r - a_1^4 > 0.$$

Now notice that if $f(x) = x^3 - x^2 + (x + 1)r$, then f is an increasing function of $x \in \mathbb{R}$ (since $r \geq 2$) and has its real root a_1 between -1 and 0, since $f(-1) = -2$ and $f(0) = r$. However, for these constraints on a_1, we then see that

$$c > r^2 - r - 1 > 0,$$

again since $r \geq 2$.

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

Now let $L = K(a_1)$, so $L \subset \mathbb{R}$ and $[L : K] \leq 3$. Moreover, $\beta = a_1\alpha + a_1\alpha^2 - \alpha^3 + \alpha^4$ and satisfies the equation $x^5 + ax + b = 0$, where $a, b \in L$, with $a > 0$ by construction and $b \neq 0$. Also notice that $L(\alpha) = L(\beta)$. This establishes the proposition. □

Now we can complete the proof of Theorem 6.

Proof of Theorem 6. Let $r \in \mathbb{F}$ and assume, without loss of generality, that $r \geq 2$. Hence $r \in K_n$ for some real q-tower $K_0 \subseteq \cdots \subseteq K_n$ of $\mathbb{Q}$. Consider the field $K_n(\sqrt[5]{r})$. If $[K_n(\sqrt[5]{r}) : K_n] < 5$, then $\sqrt[5]{r} \in \mathbb{F}$, since $\mathbb{F}$ is Vietian (see the proof of Proposition 5). Hence we may assume that this field extension is of degree five and thus $x^5 - r$ is irreducible in $K_n[x]$. Now by the previous proposition, there is an extension $L \subseteq \mathbb{R}$ such that $[L : K_n] \leq 3$ and there is an element β, which is the real root of a polynomial $x^5 + ax + b \in L[x]$ with $a > 0$, such that $L(\sqrt[5]{r}) = L(\beta)$. Next, let $N = L(\sqrt[4]{a})$ and let $\gamma = \beta/\sqrt[4]{a}$ where $\sqrt[4]{a}$ denotes the positive fourth root of a. Now γ is a root of the polynomial $x^5 + x + b/\sqrt[4]{a^5}$. Let $M = L(\sqrt{a})$ and $R = N(\gamma)$. However,

$$K_0 \subseteq \cdots \subseteq K_n \subseteq L \subseteq M \subseteq N \subseteq R$$

is then a real q-tower of $\mathbb{Q}$ such that $\sqrt[5]{r} \in R$, as desired. □

Notice that $x^5 - r$ has exactly one real root for $r \in \mathbb{F}$. This is no accident, as the following theorem indicates.

Theorem 8. *Let $p(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 \in \mathbb{F}[x]$ and be irreducible over $F = \mathbb{Q}(a_1, \ldots, a_5)$. If p has a root in $\mathbb{F}$, then p has exactly one real root.*

To prove this theorem we first isolate a lemma.

Lemma 9. *Let K/k be a finite Galois extension and F/k an arbitrary extension for which both K and F are subfields of some common field. If L is any field such that $F \cap K \subseteq L \subseteq K$, then the degree $[L : F \cap K] = [LF : F]$.*

Proof. As is well known, KF/F is a Galois extension and

$$\mathrm{Gal}(K/K \cap F) \simeq \mathrm{Gal}(KF/F).$$

Hence K and F are linearly disjoint over $K \cap F$; see, for instance, [5, Section 20]. However, by transitivity of linear disjointness (again see the above reference), L and F are then linearly disjoint over $K \cap F$. Thus $[L : F \cap K] = [LF : F]$, as desired. □

Now we proceed with the proof of the theorem.

Proof of Theorem 8. Write p as $\prod_{j=1}^{5}(x - \beta_j)$ where $\beta_j \in \mathbb{C}$. Let $K_0 \subseteq \cdots \subseteq K_n$ be a q-tower of minimal length such that there is a root of p contained in K_n, that is,

$$n = \min\{m : K_m \cap \{\beta_1, \ldots, \beta_5\} \neq \emptyset\}.$$

Hence K_{n-1} contains no roots of p. Let $N = F(\beta_1, \ldots, \beta_5)$ be the splitting field of p over F. (Recall that $\mathrm{Gal}(N/F)$ is isomorphic to C_5, the cyclic group of order

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

five, D_5, the dihedral group of order 10, F_{20}, the Frobenius group of order 20, A_5, the alternating group of degree five, or S_5, the full symmetric group; see [2, Section 13.2] for a particularly nice presentation of this and related facts.) We consider two cases according as the degree $[N \cap FK_{n-1} : F]$ is not or is a multiple of 5.

Case 1. Suppose that $5 \nmid [N \cap FK_{n-1} : F]$. Let $\beta = \beta_j \in K_n$. Since $[F(\beta) : F] = 5$ but $5 \nmid [N \cap FK_{n-1} : F]$, we see that $[(N \cap FK_{n-1})(\beta) : N \cap FK_{n-1}] = 5$. Hence by Lemma 9, $[FK_{n-1}(\beta) : FK_{n-1}] = 5$; and thus

$$[K_n : K_{n-1}] \geq [K_{n-1}(\beta) : K_{n-1}] \geq [FK_{n-1}(\beta) : FK_{n-1}] = 5.$$

Since $[K_n : K_{n-1}] \leq 5$ we have $[K_n : K_{n-1}] = 5$. However, this implies that K_n/K_{n-1} is an ultraradical extension and so, in particular, the minimal polynomial of any generator of K_n/K_{n-1} must have exactly one real root. Since β is such a generator and p is its minimal polynomial over K_{n-1} (as well as F), p must have exactly one real root, as desired.

Case 2. Suppose that $5 \mid [N \cap FK_{n-1} : F]$. We show that this case cannot occur. Let $G = \mathrm{Gal}(N/F)$ and consider G identified with a subgroup of S_5 by fixing an ordering of the roots of p. This ordering may be altered for convenience in what follows. We now consider the five possible groups to which G can be isomorphic.

If $G \simeq C_5$, then $N = F(\beta)$. However, $N \cap FK_{n-1} = F$, since K_{n-1} contains none of the β_j, contrary to the assumption in this case. Thus G cannot be cyclic of order five.

In the other four instances, we claim first that all the $F_j = F(\beta_j)$ are distinct. For otherwise suppose, without loss of generality, that $F_1 = F_2$. Then (see [2]) G contains a 5-cycle $\sigma = (12ijk)$. Again, without loss of generality, assume that $\sigma = (12345)$. However, we then have $F_2 = \sigma(F_1) = \sigma(F_2) = F_3$, and, furthermore, $F_3 = \sigma(F_2) = \sigma(F_3) = F_4$. Similarly $F_4 = F_5$. Thus all the F_j are identical, which implies that $G \simeq C_5$; but we have ruled this situation out. Thus these fields are distinct as claimed. Now each of the four groups D_5, F_{20}, A_5, S_5 has exactly five subgroups of index 5 in the full group. Hence $\mathrm{Gal}(N/F_j)$ must correspond to these maximal subgroups. Now since no $\beta_j \in N \cap FK_{n-1}$, we see that $\mathrm{Gal}(N/N \cap FK_{n-1}) \not\subseteq \mathrm{Gal}(N/F_j)$ for any j. However, $5 \mid [N \cap FK_{n-1} : F]$, and so the index of $\mathrm{Gal}(N/N \cap FK_{n-1})$ in G must be a multiple of 5 in G, or equivalently the order of $\mathrm{Gal}(N/N \cap FK_{n-1})$ is not divisible by 5.

If $G \simeq D_5$ or F_{20}, any subgroup whose order is not a multiple of five lies in a subgroup of index 5 in G. Thus $\mathrm{Gal}(N/N \cap FK_{n-1}) \subseteq \mathrm{Gal}(N/F_j)$ for some j, contrary to the assumption of Case 2. Hence these two groups cannot occur in this case.

Finally, suppose that $G \simeq S_5$ or A_5. First consider S_5. The five subgroups of index 5 (hence of order 24) are $S_4^{(i)} = \{\sigma \in S_5 : \sigma(i) = i\}$, for $i = 1, \ldots, 5$. There are subgroups of order relatively prime to five that are not contained in any of the $S_4^{(i)}$. They are the conjugates of $H_1 = \langle (123), (45) \rangle = \langle (123)(45) \rangle \simeq C_6$ and $H_2 = \langle (123), (12)(45) \rangle \simeq S_3$, which are of order six, and $H_3 = \langle (123), (12), (45) \rangle \simeq S_3 \times S_2$ of order 12. It turns out that H_3 is a maximal subgroup of S_5 and H_3 is the only subgroup lying between S_5 and either of H_1 and H_2. Similarly for A_5, H_2 above is a maximal subgroup (unique up to conjugation) in A_5 not contained in any of the subgroups of index 5 in A_5.

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

Now let $H = \mathrm{Gal}(N/N \cap FK_{n-1})$. Then H must be conjugate to H_1, H_2 or H_3 in S_5 if $G \simeq S_5$, or to H_2 in A_5 if $G \simeq A_5$. If $G \simeq S_5$ and H is conjugate to H_3 or if $G \simeq A_5$ and H is conjugate to H_2, then $N \cap FK_{n-1}/F$ is of degree 10 with no intermediate subfields. In the other two situations, $[N \cap FK_{n-1} : F] = 20$ and $N \cap FK_{n-1}/F$ contains exactly one intermediate field K and $[K : F] = 10$.

Now let k be the maximal index such that $N \cap FK_k = F$. Since

$$F \subset N \cap FK_{k+1} \subseteq N \cap FK_{n-1},$$

we see that $[N \cap FK_{k+1} : F] \geq 10$. First suppose that $[N \cap FK_{n-1} : F] = 10$. Thus $N \cap FK_{n-1} = N \cap FK_{k+1}$. However, by Lemma 9, we then have

$$[(N \cap FK_{n-1})FK_k : FK_k] = [N \cap FK_{n-1} : F] = 10.$$

However,

$$FK_k \subset (N \cap FK_{k+1})FK_k \subseteq FK_{k+1}$$

and thus

$$[K_{k+1} : K_k] \geq [FK_{k+1} : FK_k] \geq 10,$$

which contradicts the definition of a q-tower. On the other hand, suppose now that $[N \cap FK_{n-1} : F] = 20$. Again, let K be the unique field with $F \subseteq K \subseteq N \cap FK_{n-1}$ for which $[K : F] = 10$. Hence $N \cap FK_{k+1} = K$ or $N \cap FK_{k+1} = N \cap FK_{n-1}$ since $F \subset N \cap FK_{k+1} \subseteq N \cap FK_{n-1}$. Applying Lemma 9 again, we see that

$$[(N \cap FK_{k+1})FK_k : FK_k] \geq 10.$$

However,

$$FK_k \subset KFK_k \subseteq (N \cap FK_{k+1})FK_k \subseteq FK_{k+1},$$

and so $[K_{k+1} : K_k] \geq 10$, which cannot occur.

This establishes the theorem. □

We can say more, namely, the converse of this theorem is also true.

THEOREM 10. *Let*

$$p(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 \in \mathbb{F}[x]$$

and be irreducible over $F = \mathbb{Q}(a_1, \ldots, a_5)$. *If* p *has exactly one real root, then this real root is in* $\mathbb{F}$.

A major part of the proof of this theorem (in a different context) was given by Sylvester using an application of an extension of his law of inertia for quadratic forms. Here is one version of Sylvester's result, stated in a way that will be convenient.

THEOREM 11. *Let*

$$p(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 \in F[x]$$

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

with exactly one real root, β, where F be a subfield of $\mathbb{R}$. Then there are field extensions

$$F \subseteq K \subseteq L \subseteq M \subseteq \mathbb{R}$$

such that $[K : F] \leq 2$, $[L : K] \leq 2$ and $[M : L] \leq 3$ such that $M(\beta) = M(\gamma)$ where γ is a root of a polynomial $q(x) = x^5 - ax - b$ for some $a, b \in M$.

For a proof, see [7]. A similar theorem is true if there is no restriction on the reality of the coefficients. This follows by the (independent) work of Bring and Jerrard as is well known. Sylvester's contribution was in considering the real case.

Before proving Theorem 10, we single out a result; but first we give a couple of definitions. Let

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = a_0 \prod_{i=1}^{n}(x - x_i)$$

and

$$g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m = b_0 \prod_{i=1}^{m}(x - y_i)$$

be polynomials over some field. Then the discriminant of f is

$$D(f) = a_0^{2n-2} \prod_{i<j}(x_i - x_j)^2,$$

and the resultant of f and g is

$$R(f, g) = a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m}(x_i - y_j).$$

Proposition 12. *Let f and g be polynomials with real coefficients of degrees three and four respectively, such that $a_0 > 0$ and $b_0 > 0$.*

(1) *If $D(f) < 0$, then exactly one root of f is real.*
(2) *If $D(g) < 0$, then exactly two (distinct) roots of g are real.*
(3) *Suppose that $D(f) < 0$ and $D(g) < 0$. Without loss of generality, let $x_1 \in \mathbb{R}$ and $y_1, y_2 \in \mathbb{R}$ with $y_1 < y_2$. If $R(f, g) < 0$, then $y_1 < x_1 < y_2$, in which case $g(x_1) < 0$.*

Proof. The statements (1) and (2) are well known (see for example [9, pp. 272–277]). Thus we prove only (3). First,

$$R(f, g) = a_0^4 b_0^3 (x_1 - y_1)(x_1 - y_2)z,$$

where

$$z = (x_1 - y_3)(x_1 - y_4) \prod_{i=2}^{3} \prod_{j=1}^{4}(x_i - y_j).$$

However, the factors appearing in z come in complex conjugate pairs, and so $z > 0$. Further, $(x_1 - y_1)(x_1 - y_2) < 0$ since $R(f, g) < 0$ and $a_0, b_0 > 0$. It now follows that $y_1 < x_1 < y_2$, and hence $g(x_1) < 0$. □

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

Now we prove Theorem 10.

Proof of Theorem 10. It suffices to prove the theorem for $p(x) = x^5 - ax - b$, by Sylvester's result above. Notice that the case where $a = 0$ follows from Theorem 6. Hence we assume that $a \neq 0$ and consider two cases, according to the sign of a.

Case 1. Suppose that $a < 0$. Let β be the unique real root of p. If $c \in \mathbb{R} \setminus \{0\}$, then, since $\beta^5 - a\beta - b = 0$, multiplying this equation by c^5, we see that

$$(c\beta)^5 - ac^4(c\beta) - c^5 b = 0.$$

Now let $c = 1/\sqrt[4]{|a|}$, where $\sqrt[4]{|a|}$ is one of the real fourth roots of $|a|$. Hence $\beta/\sqrt[4]{|a|}$ satisfies $q(x) = x^5 + x - b/\sqrt[4]{|a^5|} = 0$. Since $|a|^{1/4} \in \mathbb{F}$ and thus also $q(x) \in \mathbb{F}[x]$, we see that $\beta/|a|^{5/4} \in \mathbb{F}$. However, we then have $\beta \in \mathbb{F}$, as desired.

Case 2. Suppose that $a > 0$. The argument in Case 1 then shows that we may assume, without loss of generality, that $p(x) = x^5 - x - b$. We now follow Bring and Jerrard, and Sylvester, by introducing a (real) Tschirnhaus transformation to transform $p(x) = x^5 - x - b$ into $q(y) = y^5 - a_1 y - b_1$, where $a_1 < 0$ and a_1 and b_1 are in the appropriate field extension of $F = \mathbb{Q}(b)$. To this end, let $p(x) = x^5 - x - b = \prod_{i=1}^{5}(x - x_i)$, where $x_i \in \mathbb{C}$ are the roots of p. Recall that the discriminant Δ of p is $5^5 b^4 - 2^8$. Since p is irreducible, hence separable, $\Delta \neq 0$. Moreover, since p has exactly one real root, $\Delta > 0$; see [2, 9]. Let

$$y = u_0 + u_1 x + u_2 x^2 + u_3 x^3 + u_4 x^4,$$

where $u_i \in \mathbb{R}$ are to be determined so that

$$q(y) = y^5 - a_1 y - b_1 = \prod_{i=1}^{5}(y - y_i),$$

where $y_i = \sum_{\mu=0}^{4} u_\mu x_i^\mu$.

Now the coefficients of the polynomials can be expressed in terms of elementary symmetric functions of their roots. However, the coefficients may also be given in terms of power sums of their roots, and for us this will be more convenient, as before. For a nonnegative integer k, let

$$s_k = \sum_{i=1}^{5} x_i^k \quad \text{and} \quad s'_k = \sum_{i=1}^{5} y_i^k.$$

Once again we recall Newton's identities. Let

$$f(x) = x^n + c_1 x^{n-1} + \cdots + c_n = \prod_{i=1}^{n}(x - x_i),$$

and, for all positive integers m, let

$$s_m = \sum_{i=1}^{n} x_i^m.$$

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

Then

$$s_m + c_1 s_{m-1} + \cdots + c_{m-1} s_1 + m c_m = 0,$$

where we define $c_m = 0$ for all $m > n$. From this we can determine the s_m recursively.

Again consider $p(x) = x^5 - x - b$. By Newton's identities (with $c_1 = c_2 = c_3 = 0$, $c_4 = -1$, and $c_5 = -b$), we have for $m = 1$, $s_1 + c_1 = 0$, and so $s_1 = -c_1 = 0$. For $m = 2$ we see that $s_2 + c_1 s_1 + 2c_2 = 0$ and thus $s_2 = -c_1 s_1 - 2c_2 = 0$. Similarly, $s_3 = 0$, $s_4 = 4$, and $s_5 = 5b$. For $m > 5$, we see easily that

$$s_m = s_{m-4} + b s_{m-5}.$$

From all of this we list the first 16 power sums for later use:

$$\begin{array}{llll} s_1 = 0, & s_2 = 0, & s_3 = 0, & s_4 = 4, \\ s_5 = 5b, & s_6 = 0, & s_7 = 0, & s_8 = 4, \\ s_9 = 9b, & s_{10} = 5b^2, & s_{11} = 0, & s_{12} = 4, \\ s_{13} = 13b, & s_{14} = 14b^2, & s_{15} = 5b^3, & s_{16} = 4. \end{array}$$

Also recall that $q(y) = \prod_{i=1}^{5}(y - y_i)$. We first write

$$q(y) = y^5 + B_1 y^4 + B_2 y^3 + B_3 y^2 + B_4 y + B_5,$$

where $y_i = \sum_{\mu=0}^{4} u_\mu x_i^\mu$. We want $q(y) = y^5 - a_1 y - b_1$ as noted above, and so we need to determine the Tschirnhaus transformation such that $B_1 = B_2 = B_3 = 0$ and $B_4 > 0$.

By Newton's identities, we may determine the coefficients B_j in terms of the power sums s'_k. After this we can rewrite the s'_k and thus also the B_j in terms of u_μ and s_m (the power sums of the x_i). To this end, we first want $B_1 = 0$. By Newton's identities,

$$s'_1 + B_1 = 0$$

and hence $s'_1 = -B_1 = 0$. However, on the other hand,

$$\begin{aligned} s'_1 &= \sum_{i=1}^{5} y_i = \sum_{i=1}^{5} \sum_{\mu=0}^{4} u_\mu x_i^\mu = \sum_{\mu=0}^{4} u_\mu \sum_{i=1}^{5} x_i^\mu \\ &= 5u_0 + u_1 s_1 + u_2 s_2 + u_3 s_3 + u_4 s_4 = 5u_0 + 4u_4, \end{aligned}$$

from our table of values of s_m above. Hence

$$u_0 = -\tfrac{4}{5} u_4.$$

Thus in order to have $B_1 = 0$, we use the Tschirnhaus transformation:

$$y = u_1 x + u_2 x^2 + u_3 x^3 + u_4 (x^4 - \tfrac{4}{5}).$$

Next, we want $B_2 = 0$. Again using Newton's identities,

$$s'_2 + B_1 s'_1 + 2B_2 = 0,$$

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

and so $s_2' = -2B_2 = 0$ (as $B_1 = 0$). On the other hand,

$$\begin{aligned}
s_2' &= \sum_{i=1}^{5} y_i^2 = \sum_{i=1}^{5}\left(u_1x_i + u_2x_i^2 + u_3x_i^3 + u_4\left(x_i^4 - \frac{4}{5}\right)\right)^2 \\
&= \sum_{i=1}^{5}\left(u_1^2x_i^2 + u_2^2x_i^4 + u_3^2x_i^6 + u_4^2\left(x_i^8 - \frac{8}{5}x_i^4 + \frac{16}{25}\right) + 2\left(u_1u_2x_i^3 + u_1u_3x_i^4\right)\right. \\
&\qquad \left. + 2\left(u_1u_4\left(x_i^5 - \frac{4}{5}x_i\right) + u_2u_3x_i^5 + u_2u_4\left(x_i^6 - \frac{4}{5}x_i^2\right) + u_3u_4\left(x_i^7 - \frac{4}{5}x_i^3\right)\right)\right) \\
&= u_1^2s_2 + u_2^2s_4 + u_3^2s_6 + u_4^2\left(s_8 - \frac{8}{5}s_4 + \frac{16}{5}\right) + 2(u_1u_2s_3 + u_1u_3s_4) \\
&\qquad + 2\left(u_1u_4\left(s_5 - \frac{4}{5}s_1\right) + u_2u_3s_5 + u_2u_4\left(s_6 - \frac{4}{5}s_2\right) + u_3u_4\left(s_7 - \frac{4}{5}s_3\right)\right) \\
&= 4u_2^2 + u_4^2\left(4 - \frac{32}{5} + \frac{16}{5}\right) + 2(4u_1u_3 + 5bu_1u_4 + 5bu_2u_3).
\end{aligned}$$

Thus we have

$$0 = s_2' = 4u_2^2 + \tfrac{4}{5}u_4^2 + 8u_1u_3 + 10bu_1u_4 + 10bu_2u_3.$$

Notice that the right side is a quadratic form in the u_μ and can be diagonalized, as was done beautifully by Sylvester in much more generality using his extended version of his law of inertia, by completing the squares as

$$0 = s_2' = 4v_2^2 + \frac{4}{5}v_4^2 - \frac{25b^2}{4}v_3^2 - \frac{1}{100b^2}\Delta v_1^2,$$

where

$$v_1 = u_1, \quad v_2 = u_2 + \frac{5b}{4}u_3, \quad v_3 = u_3 - \frac{16}{25b^2}u_1,$$
$$v_4 = u_4 + \frac{25b}{4}u_1, \quad \text{and} \quad \Delta = 5^5b^4 - 2^8,$$

the discriminant of p as identified above. Choosing the u_μ (which we shall do later) to satisfy the above equation will then guarantee that $B_2 = 0$.

Next we want $B_3 = 0$. By Newton's identities,

$$s_3' + B_1s_2' + B_2s_1' + 3B_3 = 0,$$

in which case we see that $s_3' = 0$. On the other hand,

$$s_3' = \sum_{i=1}^{5} y_i^3 = \sum_{i=1}^{5}\left(\sum_{\mu=0}^{4} u_\mu x_i^\mu\right)^3.$$

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

Expanding in a manner similar to that in the case of s_2' above, one finds that

$$0 = s_3' = -\tfrac{12}{25}u_4^3 + 9bu_3^3 + 3bu_1u_4^2 + 15b^2u_2u_4^2 + 15b^2u_3^2u_4 + 12u_2u_3^2 + \tfrac{12}{5}u_2^2u_4 + 15bu_1u_2^2 + 15bu_1^2u_3 + 12u_1^2u_2 + \tfrac{24}{5}u_1u_3u_4 + 30bu_2u_3u_4.$$

Finally, we need to consider B_4, which we want to be positive. Again by Newton's identities, we easily see that $s_4' = -4B_4$, and thus we wish to have $s_4' < 0$. In the same manner as for s_2' and s_3', one finds that s_4' is equal to

$$\begin{aligned}&\tfrac{52}{125}u_4^4 + (20b^3u_3 + 8b^2u_2 + 4bu_1)u_4^3\\ &\quad + (36b^2u_3^2 + \tfrac{108}{5}bu_2u_3 + \tfrac{48}{25}u_1u_3 + \tfrac{24}{25}u_2^2 + 30b^2u_1^2)u_4^2\\ &\quad + (\tfrac{116}{5}bu_3^3 + \tfrac{48}{5}u_2u_3^2 + 120b^2u_1u_2u_3 + 20b^2u_2^3 + 60bu_1^2u_3 + 60bu_1u_2^2 + \tfrac{48}{5}u_1^2u_2)u_4\\ &\quad + (4u_3^4 + 20b^2u_1u_3^3 + 30b^2u_2^2u_3^2 + 108bu_1u_2u_3^2 + 36bu_2^3u_3 + 24u_1^2u_3^2 + 48u_1u_2^2u_3\\ &\quad + 4u_2^4 + 20bu_1^3u_2 + 4u_1^4).\end{aligned}$$

We are now in a position to choose the u_μ so that $s_2' = s_3' = 0$ and (perhaps miraculously) $s_4' < 0$. We start by letting

$$v_2 = \frac{5}{4}bv_3 \quad \text{and} \quad v_4 = \frac{\sqrt{5\Delta}}{20b}v_1,$$

in which case it is guaranteed that $s_2' = 0$. In terms of the u_μ we see that

$$u_2 = \omega_2 u_1 \quad \text{and} \quad u_4 = \omega_4 u_1,$$

with

$$\omega_2 = -\frac{4}{5b} \quad \text{and} \quad \omega_4 = \frac{\sqrt{5\Delta} - 5^3b^2}{20b}.$$

Notice that u_1 and u_3 are still arbitrary.

Now write $u_3 = \omega_3 u_1$ and compute s_3' with $u_\mu = \omega_\mu u_1$ for $\mu = 2, 3, 4$. Since s_3' is a homogeneous form of degree three in $u_1, \ldots, u_4$, we see that u_1^3 is a factor of s_3'. A straightforward calculation yields

$$\frac{s_3'}{3bu_1^3} = 3\omega_3^3 + A_1\omega_3^2 + A_2\omega_3 + A_3,$$

where the $A_i = A_i(\Delta)$ are given by

$$\begin{aligned}A_1 &= -\frac{16}{5b^2} + \frac{\sqrt{5\Delta} - 5^3b^2}{4} = -\sqrt{5}\Big(\frac{144}{\sqrt{256+\Delta}} + \frac{\Delta}{4\sqrt{256+\Delta}} - \frac{\sqrt{\Delta}}{4}\Big),\\ A_2 &= 45 - \frac{8\sqrt{5\Delta}}{25b^2} = 5\Big(9 - \frac{8\sqrt{\Delta}}{\sqrt{256+\Delta}}\Big),\\ A_3 &= -\Big(\frac{\sqrt{5\Delta} - 5^3b^2}{20b}\Big)^2\Big(2 + \frac{\sqrt{5\Delta}}{5^3b^2}\Big) + \frac{16}{5^4b^4}(\sqrt{5\Delta} - 5^3b^2)\\ &= -5^{3/2}\Big(\frac{2^{12}(2\sqrt{\Delta} + 3\sqrt{256+\Delta})}{(256+\Delta)(\sqrt{\Delta} + \sqrt{256+\Delta})^2}\Big).\end{aligned}$$

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

Notice that we have given these coefficients in terms of Δ simply by solving for b, which we assume positive without loss of generality. Hence if $\omega_3 = \omega_3(\Delta)$ is a real root of the polynomial

$$f(x) = f_\Delta(x) = 3x^3 + A_1x^2 + A_2x + A_3,$$

then $B_3 = 0$.

On the other hand, again letting $u_\mu = \omega_\mu u_1$ for $\mu = 2, 3, 4$ and then setting $x = \omega_3$ one finds that

$$\frac{s_4'}{u_1^4} = g(x) = g_\Delta(x) = 4x^4 + C_1x^3 + C_2x^2 + C_3x + C_4,$$

with $C_i = C_i(\Delta)$ given as

$$\begin{aligned}
C_1 &= \left(\frac{29}{25}\sqrt{\Delta} - \sqrt{256+\Delta}\right)\sqrt{5},\\
C_2 &= 120 + \frac{9}{10}\Delta - \frac{1392\sqrt{\Delta}}{5\sqrt{256+\Delta}} - \frac{9\Delta^{3/2}}{10\sqrt{256+\Delta}},\\
C_3 &= \frac{87}{\sqrt{5}}\sqrt{\Delta} + \frac{\Delta^{3/2}}{4\sqrt{5}} - \frac{1280\sqrt{5}}{\sqrt{256+\Delta}} - \frac{119\Delta}{\sqrt{5}\sqrt{256+\Delta}} - \frac{\Delta^2}{4\sqrt{5}\sqrt{256+\Delta}},\\
C_4 &= \frac{25600}{256+\Delta} + \frac{852\Delta}{256+\Delta} + \frac{25\Delta^2}{8(256+\Delta)} - \frac{464\sqrt{\Delta}}{\sqrt{256+\Delta}} - \frac{25\Delta^{3/2}}{8\sqrt{256+\Delta}}.
\end{aligned}$$

We shall be done essentially if we can show that $g(\omega_3) < 0$. To get a hint as to how to proceed we looked numerically at data involving f and g for $\Delta \geq 0$. For $\Delta = 0$ (which is, of course, contrary to our assumption), $f(x) = 3(x - \sqrt{5})^3$ and $g(x) = 4(x - \sqrt{5})^4$ and thus f and g have the same unique root. On the other hand, for all the positive values of Δ that we checked, g had exactly two real roots, while f had a unique real root that was sandwiched between the two real roots of g. This, of course, implies that $g(\omega_3) < 0$ in these cases. To actually prove these facts, in light of Proposition 12 it suffices to show that for all $\Delta > 0$, the discriminants of f and g are negative and that the resultant of f and g is also negative. To evaluate these quantities symbolically, we used MATHEMATICA.

The discriminant of f_Δ is found to be

$$D(f) = \frac{125}{32(256+\Delta)^{5/2}}(A - B),$$

where

$$A = 387\Delta^{1/2} + 2\Delta^{3/2} \quad \text{and} \quad B = (131 + 2\Delta)\sqrt{256+\Delta}.$$

However, $D(f) < 0$ if and only if $B^2 - A^2 > 0$. Moreover,

$$B^2 - A^2 = 1536\Delta + 4393216 > 0,$$

as desired.

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

Next we found the discriminant of g to be

$$D(g) = \frac{27\Delta^6}{31250(256+\Delta)^3}(C-D),$$

where

$$C = (50697 + 1036\Delta + 4\Delta^2)\sqrt{\Delta}\sqrt{256+\Delta},$$
$$D = 2196608 + 150537\Delta + 1548\Delta^2 + 4\Delta^3.$$

Hence $D(g) < 0$ if and only if $D^2 - C^2 > 0$. However,

$$D^2 - C^2 = 589824\Delta^2 + 3373989888\Delta + 4825086705664 > 0,$$

as desired.

We now consider the resultant of f and g. This turns out to be

$$R(f,g) = \frac{\Delta^6}{k\sqrt{256+\Delta}}(E-F),$$

where

$$E = (m_0 + m_1\Delta + \cdots + m_7\Delta^7)\sqrt{\Delta}$$
$$F = (n_0 + n_1\Delta + \cdots + n_7\Delta^7)\sqrt{256+\Delta},$$

where k, the m_j and the n_j are given in Table 1. Hence $R(f,g) < 0$ if and only if $F^2 - E^2 > 0$. However, it turns out that

$$F^2 - E^2 = k_0 + k_1\Delta + \cdots + k_{11}\Delta^{11},$$

where the k_j are also given in Table 1. Notice that these coefficients are all positive, as desired.

Finally we can show that the unique real root, x_1 say, of $p(x) = x^5 - x - b$ is q-constructible. This will be done by showing that x_1 lies in a q-tower of $\mathbb{Q}$. To this end, notice that since $b \in \mathbb{F}$, there exists a q-tower of $\mathbb{Q}$, say $K_0 \subseteq \cdots K_n$, for which $b \in K_n$. If p is reducible over K_n, then $x_1 \in \mathbb{F}$, being the real root of a polynomial over K_n of degree at most four, for recall that $\mathbb{F}$ is Vietian. Hence we assume that p is irreducible over K_n. Now let

$$u_1 = 1, \quad u_2 = -\frac{4}{5b}, \quad u_4 = \frac{\sqrt{5\Delta} - 5^3b^2}{20b},$$

and $u_3 = \omega_3 = \omega_3(\Delta)$ be the real root of f_Δ. Notice that

$$f_\Delta \in \mathbb{Q}(b, \sqrt{5\Delta})[x] \quad \text{and} \quad \mathbb{Q}(u_1, \ldots, u_4) = \mathbb{Q}(b, \sqrt{5\Delta}, \omega_3).$$

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

Table 1. Relevant coefficients.

k	32 768 000 000
m_0	14 269 936 894 300 127 232 000 000
m_1	570 317 780 839 038 976 000 000
m_2	8 998 789 708 775 424 000 000
m_3	74 991 638 937 600 000 000
m_4	362 223 042 560 000 000
m_5	1 023 543 552 000 000
m_6	1 575 936 000 000
m_7	1 024 000 000
n_0	2 415 196 037 665 783 808 000 000
n_1	203 254 619 999 043 584 000 000
n_2	4 509 367 768 449 024 000 000
n_3	46 721 862 205 440 000 000
n_4	264 570 961 920 000 000
n_5	846 989 568 000 000
n_6	1 444 864 000 000
n_7	1 024 000 000
k_0	1 493 292 006 491 264 562 842 625 502 974 715 101 184 000 000 000 000
k_1	53 542 746 396 833 318 735 872 129 176 912 789 504 000 000 000 000
k_2	857 182 471 590 562 824 743 459 659 626 577 920 000 000 000 000
k_3	8 056 613 010 345 157 895 879 306 206 248 960 000 000 000 000
k_4	49 136 561 411 116 580 536 626 519 736 320 000 000 000 000
k_5	202 673 055 899 025 936 195 212 279 808 000 000 000 000
k_6	570 656 643 744 086 383 518 549 968 000 000 000 000
k_7	1 078 586 086 986 262 008 299 520 000 000 000 000
k_8	1 304 721 582 145 362 984 960 000 000 000 000
k_9	916 870 188 991 774 720 000 000 000 000
k_{10}	310 178 243 149 824 000 000 000 000
k_{11}	38 654 705 664 000 000 000 000

Now let

$$y_1 = x_1 - \frac{4}{5b}x_1^2 + \omega_3(\Delta)x_1^3 + \frac{\sqrt{5\Delta} - 5^3b^2}{20b}\left(x_1^4 - \frac{4}{5}\right) \in \mathbb{Q}(b, \sqrt{5\Delta}, \omega_3, x_1). \tag{3}$$

By our construction, y_1 is the real root of $q(y) = y^5 + B_4y + B_5$, where $B_4 > 0$ and $B_4, B_5 \in \mathbb{Q}(b, \sqrt{5\Delta}, \omega_3)$. However, $y_1/B_4^{1/4}$ is then the real root of $y^5 + y + B_5/B_4^{5/4}$, that is,

$$y_1 = -B_4^{1/4}\sqrt[*]{B_5B_4^{-5/4}}.$$

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press

Hence we have a q-tower

$$K_0 \subseteq \cdots \subseteq K_n \subseteq K_n(\sqrt{5\Delta}) \subseteq K_n(\sqrt{5\Delta}, \omega_3) \subseteq K_n(\sqrt{5\Delta}, \omega_3, \sqrt{B_4}) \subseteq L \subseteq M,$$

where $L = K_n(\sqrt{5\Delta}, \omega_3, \sqrt[4]{B_4})$ and $M = L(\sqrt[5]{B_5 B_4^{-5/4}})$ with $y_1 \in M$. Now observe that $L(y_1) \subseteq L(x_1)$; but $[K_n(x_1) : K_n] = 5$ and since $[L : K_n] \mid 24$ as seen by the q-tower, hence is relatively prime to 5, $[L(x_1) : L] = 5$. However, from Equation (3) above, $y_1 \notin L$. Thus $L(x_1) = L(y_1)$ and so $x_1 \in M \subseteq \mathbb{F}$, as desired. □

5. Some comments and questions

In case it is not obvious to the reader, we note that q-constructibility cannot possibly coincide with that of a compass and a twice-notched straightedge. For example, the three real roots of the irreducible (2-Eisenstein) polynomial

$$x^5 - 4x^4 + 2x^3 + 4x^2 + 2x - 6 \in \mathbb{Q}[x]$$

are constructible with compass and marked ruler (see [1]), but are not q-constructible by Theorem 8 above.

Secondly, even though extracting fifth roots is a q-constructible process, 'q-quinsecting' angles is generally not. In particular, q-quinsecting a 90° angle requires q-constructing an 18° angle. However, if $\theta = 2\cos 18°$, then θ is a root of the polynomial $x^5 - 5x^3 + 5x - 4$, which is easily seen to be irreducible over $\mathbb{Q}$ with five real roots.

Next, notice that we restricted the compass to pass through the origin and have center on the x-axis, in order to deal with fairly simple polynomials of degree at most five. Had we used an unrestricted compass instead, then we still could not have constructed all possible numbers arising from compass and marked ruler. For the intersection of a circle and $y = x^3$ can have at most four points, but on the other hand it is possible to construct the roots of irreducible polynomials of degree at least five with more than four real roots.

On the other hand, if we replace $y = x^3$ by other cubic curves, either of genus zero again or elliptic curves, is it possible to characterize the numbers constructible using any one of these curves, along with a straightedge and (unrestricted) compass? Is it possible too that for some cubic curve, this construction process produces the same set of points as that of compass and marked ruler?

Acknowledgements

The second-named author would like to thank his son-in-law, Todd Berry, for using his free time to set up various software programs, including MATHEMATICA, on the author's laptop. MATHEMATICA was especially useful for the latter part of this paper. *Thank you, Todd!*

This manuscript is an extension of the first author's Master of Arts thesis at the University of Maine.

References

[1] A. Baragar, 'Constructions using a compass and twice-notched straightedge', *Amer. Math. Monthly* **109** (2002), 151–164.
[2] D. Cox, *Galois Theory* (Wiley Interscience, Hoboken, NJ, 2004).
[3] D. Dummit and R. Foote, *Abstract Algebra*, 2nd edn (Prentice Hall, Englewood Cliffs, NJ, 1999).
[4] G. E. Martin, *Geometric Constructions* (Springer, New York, 1998).
[5] P. Morandi, *Field and Galois Theory*, Graduate Texts in Mathematics, 167 (Springer, New York, 1996).
[6] J. Robertson, 'A variation on geometric constructions', MA Thesis, University of Maine, Orono, December 2010.
[7] J. J. Sylvester, 'On the so-called Tschirnhausen transformation', *J. reine angew. Math.* **1887**(100) (1887), 465–486.
[8] C. R. Videla, 'On points constructible from conics', *Math. Intelligencer* **19** (1997), 53–57.
[9] H. Weber, *Lehrbuch der Algebra*, 2nd edn, Vol. 1 (F. Vieweg, Braunschweig, 1898).

J. ROBERTSON, 1807 County Road, New Limerick, Maine 04761, USA
e-mail: james.robertson@umit.maine.edu

C. SNYDER, Department of Mathematics and Statistics, University of Maine, Orono, Maine 04469, USA
e-mail: snyder@math.umaine.edu

https://doi.org/10.1017/S1446788711001443 Published online by Cambridge University Press