Research Article

On the Constructibility of Real 5th Roots of Rational Numbers with Marked Ruler and Compass

Elliot Benjamin

Mathematics Department, CALCampus, NH 03461, USA

Correspondence should be addressed to Elliot Benjamin, ben496@prexar.com

Received 28 March 2012; Accepted 19 April 2012

Academic Editors: W. de Graaf and S. Raianu

We demonstrate that there are infinitely many real numbers constructible by marked ruler and compass which are unique real roots of irreducible quintic polynomials over the field of rational numbers. This result can be viewed as a generalization of the historical open question of the constructibility by marked ruler and compass of real 5th roots of rational numbers. We obtain our results through marked ruler and compass constructions involving the intersection of conchoids and circles, and the application of number theoretic divisibility criteria.

1. Introduction

One of the most perplexing perpetual problems in mathematics involves the feasibility of geometrically constructing real 5th roots of rational numbers with a compass and a straightedge with two marks, one unit apart that we will refer to as a marked ruler. This problem stems back thousands of years to the ancient Greeks, who understood that various geometric constructions, such as trisecting any given angle, duplicating any given cube, and constructing the real cube roots of rational numbers that were not perfect cubes, were not feasible to do with compass and (unmarked) straightedge [1]. The formal mathematical proof that the cube roots of nonperfect cube numbers are not constructible with straightedge and compass was given fairly recently in the context of the characterization of towers of number fields of degree 2 for each iterated field extension (see, e.g., [2, page 144]). However, the ancient Greeks extended their assortment of construction tools to allow for intersections of conic sections as well as constructions with marked ruler and compass, which enabled them to have confidence that the above "cubic" problems could all be solved using either of these two extended constructions (see, e.g., [3, 4]).

The mathematical proof of these results involving towers of number fields extends the degrees of the iterated field extensions (see above) to degree 2 or 3 [3, 4]. However, there

is a hierarchy to the relative strengths of geometric constructions involving straightedge and compass, intersections of conic sections, and marked ruler and compass. It can be readily seen that anything constructible by straightedge and compass is constructible by intersections of conic sections, and it has been proved that anything constructible by intersections of conic sections is constructible by marked ruler and compass [3]. Furthermore, by the above iterated field tower extensions of degrees 2 or 3 result, we know that it is not possible to construct 5th roots of rational numbers (that are not perfect quintic powers) by intersections of conic sections. This leads to the open question of is it possible to construct the real 5th root of a rational number that is not a perfect quintic power, by marked ruler and compass.

We let Q denote the field of rational numbers, R the reals, we stipulate that a complex number $x + yi$ is a constructible number if the point (x, y) is a constructible point (see Martin [1] for the details of constructible points and numbers), we let the symbol "C" denote containment, and from this point on the phrase "real 5th roots of rational numbers" will mean that these rational numbers are not perfect quintic powers. From Baragar [3] we can state the following lemma.

Lemma 1.1. *A complex number which is constructible by marked ruler and compass belongs to a field K that lies in a tower of fields $Q = K_0 C K_1 C K_2 C \cdots K_n = K$ for which the index $[K_j : K_{j-1}]$ at each step is 2, 3, 5, or 6; in particular if $N = [K : Q]$ then the only primes dividing N are 2, 3, or 5.*

However, it is not known if the converse of this result holds, and hence the problem of the constructibility of real 5th roots of rational numbers by marked ruler and compass is still an entirely open problem. In this paper we pursue this question by thinking of the real 5th root of a rational number as the unique real root of an irreducible quintic polynomial over the rationals. In particular we explore a generalization of the real 5th root of a rational number in this context by studying irreducible quintic polynomials over the rationals that have unique real roots and are obtained by marked ruler and compass construction. We will demonstrate that there are infinitely many numbers of this form, which is consistent with the feasibility of constructing the real 5th roots of rational numbers by marked ruler and compass. However, none of the numbers we obtain in this manner are 5th roots of rational numbers, and thus our result serves predominantly to motivate the continued exploration of this intriguing problem.

2. Q-Constructible Numbers and Unique Real Roots of Irreducible Quintic Polynomials over the Rationals

In Robertson and Snyder [5], a set of constructible numbers is given that includes the set of real roots of irreducible quintic polynomials over the rationals that have unique real roots. Robertson and Snyder [5] refer to this set of constructible numbers as "q-constructible numbers" and they give the following explicit instructions to construct them.

They initially call a point in $R \times R$, 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 it is obtained 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 the 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 describe in (ii).

A real number is called q-constructible if it is the x-coordinate of a q-constructible point lying on the x-axis, and Robertson and Snyder demonstrate that the set of q-constructible numbers is a subfield of R, the field of real numbers. Robertson and Snyder [5] give the following characterization of q-constructible numbers.

Lemma 2.1. *A real number is q-constructible if and only if there exists a sequence of field extensions $K_0 C K_1 C \cdots K_n$ with a in K_n such that $Q = K_0 C K_1 C \cdots K_n C R$, where $[K_j : K_{j-1}]$ is in $\{1, 2, 3, 5\}$ for all $j = 1, 2, \ldots, n$, and if $[K_j : K_{j-1}] = 5$ then $K_j = K_{j-1}({}^*a_{j-1})$ where a_{j-1} is in K_{j-1} and ${}^*a_{j-1}$ is the unique real root of the polynomial $x^5 + x - a_{j-1}$.*

note

In Robertson and Snyder [5, page 105], a_{j-1} instead of ${}^*a_{j-1}$ is unintentionally referred to as the unique real root of the polynomial $x^5 + x - a_{j-1}$.

Robertson and Snyder [5] demonstrate that the real 5th roots of q-constructible numbers are q-constructible, which of course implies that real 5th roots of all rational numbers are q-constructible. Furthermore, they demonstrate a more generic relationship between q-constructible numbers and irreducible quintic polynomials with q-constructible numbers as coefficients that have unique real roots over the field of rational numbers with these coefficients adjoined. For our purposes we state the part of this relationship that we are most interested in as the following lemma.

Lemma 2.2. *The field of q-constructible numbers contains the real roots of all irreducible quintic polynomials over the rationals that have unique real roots, and if a q-constructible number is a real root of an irreducible quintic polynomial $p(x)$ over the rationals, then $p(x)$ has a unique real root.*

Proof. See Robertson and Snyder [5, Theorems 3 and 4]. □

In regard to the relationship of q-constructible numbers to constructions by marked ruler and compass, Robertson and Snyder [5] point out that these two sets cannot coincide, based upon Baragar's [3] demonstration that the three real roots of the polynomial $x^5 - 4x^4 + 2x^3 + 4x^2 + 2x - 6$, which is irreducible over Q, are constructible by marked ruler and compass. However, Robertson and Snyder [5, page 104] conjecture that q-constructible numbers are contained in the set of numbers constructible by marked ruler and compass, which would imply that the real 5th roots of all rational numbers are constructible by marked ruler and compass. Our main result (see Theorem 4.4) is consistent with Robertson and Snyder's conjecture, as we demonstrate that there are infinitely many numbers constructible by marked ruler and compass that are unique real roots of irreducible quintic polynomials over the rationals, and consequently are q-constructible numbers. However, we also demonstrate (see Theorem 4.3) that there are infinitely many real numbers constructible by marked ruler and compass that are real roots of irreducible quintic polynomials over the rationals that have three real roots, which implies by Lemma 2.2 that they are not q-constructible numbers. Furthermore, none of the numbers in our set of q-constructible numbers that we obtain in Theorem 4.4 are 5th roots of rational numbers, and consequently the constructibility of real 5th roots of rational numbers by marked ruler and compass in still an entirely open problem.

3. Conchoid Marked Ruler and Compass Constructions

To obtain infinitely many real numbers constructible by marked ruler and compass that are q-constructible numbers (Theorem 4.4), as well as infinitely many real numbers constructible by marked ruler and compass that are not q-constructible numbers (Theorem 4.3), we make use of the conchoids formulation for marked ruler and compass construction given by Baragar (see [3, page 157] for a geometric illustration of the conchoid construction).

In accordance with Baragar [3, page 159], we start with a point O and we construct a conchoid as follows. Without loss of generality we assume that point O is the origin and that we construct the vertical line $x = a$, where a is a real number constructible by straightedge and compass, which has the polar equation $r = a(\sec(B))$ for any angle B. We now take a twice-notched straightedge, which is a straightedge with two notches one unit apart (which we will refer to as "ruler" for short). If we place one notch of our ruler on the given line and make the ruler pass through O, then as the designated notch traverses the line, we trace out one of the two curves whose polar equations are $r = a(\sec(B)) + 1$ or $r = a(\sec(B)) - 1$, where the choice of $+1$ or -1 depends on whether or not the line is between the second notch and the origin.

Converting to rectangular coordinates, we get $r(\cos(B)) = a + \cos(B)$ or $r(\cos(B)) = a - \cos(B)$. As Baragar [3, pages 159-160], demonstrates, the equation becomes $(x - a)^2 (x^2 + y^2) = x^2$, and when we intersect the conchoid with the circle $(x - b)^2 + (y - c)^2 = s^2$, where b, c, and s are real numbers constructible by straightedge and compass, we obtain the equation $(x - a)^2 (s^2 + 2bx + 2cy - b^2 - c^2) = x^2$. Baragar [3, page 160] writes the equation in the form $yA(x) = B(x)$ where $A(x)$ and $B(x)$ are of degree 2 and degree 3, respectively, and obtains the following degree 6 equation, which we refer to as follows:

$$(A(x))^2 \left(s^2 - (x - b)^2\right) - (B(x) - cA(x))^2 = 0. \tag{3.1}$$

In the next section we make use of the above conchoid equation derived from the marked ruler and compass construction to obtain our families of irreducible quintic polynomials over the rationals that illustrate our results that we formulate as Theorems 4.3 and 4.4.

4. Irreducible Quintic Polynomials from Conchoid Marked Ruler and Compass Constructions

In order to obtain quintic polynomials from (3.1), which is a degree 6 equation, we construct families with the particular requirements that $c = s$ and either $b = a + 1$ or $b = a - 1$.

It readily follows that $(b, 0)$ is a point of intersection of the conchoid and circle described in Section 3, and satisfies Equation (3.1). If we stipulate that a is a rational number, then we see that (3.1) factors over the rationals into a linear factor and a quintic polynomial factor.

In order to obtain families in which these quintic polynomial factors are irreducible over the rationals, we make use of two well-known number theory tests for irreducibility of polynomials.

Our first irreducibility test is the Einsenstein criterion (see, e.g., [2, Proposition 5.3, page 235], which for our purposes we utilize the following part of.

Lemma 4.1. *Let D be a unique factorization domain with quotient field F, and let $f(x) = a_0 + a_1x + a_2x^2 + \cdots a_nx^n$ be in $D[x]$. Suppose there is a prime element p in D such that p divides $a_0, a_1, \ldots, a_{n-1}$ but not a_n, and that p^2 does not divide a_0. Then f is irreducible over F.*

Our second irreducibility test involves moding out by prime ideals (see, e.g., [6, Theorem 6.11, page 150]), which we state in the following format.

Lemma 4.2. *Let D be a unique factorization domain with quotient field F, and let $f(x)$ in $D[x]$ be such that the content of $f(x)$ (i.e., the greatest common divisor of the coefficients of $f(x)$) is 1. If p in D is a prime element such that p does not divide the leading coefficient a_n of $f(x)$, and if $f(x)(\mathrm{mod}(p))$ is irreducible in $(D/(p))[x]$, then f is irreducible over F.*

We now demonstrate that there are infinitely many real numbers constructible by marked ruler and compass that are not q-constructible. To this end we let $a = 2$, $b = 1$, and $c = s$ in the conchoid and circle construction described in Section 3, and we obtain $A(x) = 2cx^2 - 8cx + 8c$ and $B(x) = -2x^3 + 10x^2 - 12x + 4$ in (3.1). After sorting out the algebraic details and factoring out $x - 1$, we obtain the 5th degree polynomial $(c^2 + 1)x^5 + (-7c^2 - 9)x^4 + (16c^2 + 28)x^3 + (-12c^2 - 36)x^2 + 20x - 4$. We note that if c is odd then $c^2 + 1$, the coefficient of x^5, is congruent to 2(mod 4), and all the other coefficients are congruent to 0(mod 4). When we divide all these terms by 2, we see that the Einsenstein conditions of Lemma 4.1 are satisfied, using $D = $ the integers Z, $F = $ the rationals Q, and $p = 2$, and we are thus able to conclude that our family of quintic polynomials are irreducible over Q whenever c is odd, which gives us infinitely many irreducible polynomials over Q.

For a concrete example we let $c = 15$, obtaining the irreducible quintic polynomial $113x^5 - 292x^4 + 1814x^3 - 1332x^2 + 10x - 2$, which has three real roots. Through geometric constructions of our conchoids and circles, as described in Baragar [3], we obtain for $a = 2, b = 1$, and $c = s$, that whenever $c > 1.83$ then our above quintic polynomial has three real roots. We thus conclude that for all odd integers greater than 1 we have obtained irreducible quintic polynomials that have more than one real root, and consequently from Lemma 2.2 we have proved the following result.

Theorem 4.3. *There are infinitely many real numbers constructible by marked ruler and compass that are not q-constructible.*

To prove that there are infinitely many real numbers constructible by marked ruler and compass that are unique real roots of irreducible quintic polynomials over Q and consequently q-constructible, we once again make use of the marked ruler conchoids and circle constructions described in Baragar [3] and Section 3. However, this time we study the family obtained by letting $a = -.5, b = .5$, and $c = s$ in our conchoid and circle construction described in Section 3, and we obtain $A(x) = 2cx^2 + 2cx + .5c$ and $B(x) = -x^3 + .25x^2 + .0625$ in (3.1). After sorting out the algebraic details and factoring out $x - .5$, we obtain the 5th degree polynomial $(512c^2 + 128)x^5 + 1280c^2x^4 + (896c^2 + 8)x^3 + (192c^2 + 2)x^2 - 2x - 1$.

We now stipulate that $c = d/((2^{2n})e)$ for integers d, e, and n with $n \geq 1$, d congruent to 1(mod 3) or 2(mod 3), and e congruent to 1(mod 3) or 2(mod 3). Substituting these values into our above polynomial and multiplying through by $(2^{4n})e^2$ we obtain the 5th degree polynomial $p(x) = (512d^2 + 128e^2(2^{4n}))x^5 + 1280d^2x^4 + (896d^2 + 8e^2(2^{4n}))x^3 + (192d^2 - 12e^2(2^{4n}))x^2 - e^2(2^{4n} + 1)x - e^2(2^{4n})$.

To show that our polynomial $p(x)$ is irreducible over Q, we make use of Lemma 4.2 by initially reducing $p(x)(\mathrm{mod}\ 3)$ to obtain the quintic polynomial $p_3(x) = x^5 + 2x^4 + x^3 + x + 2$,

which we readily check is irreducible over $Z(\mathrm{mod}\,3Z)$. In order to satisfy the **Lemma 4.2** condition of the content being 1, we divide the coefficients of $p(x)$ by their greatest common divisor, obtaining a quintic polynomial $p^*(x)$ with content 1. We reduce $p^*(x)$ mod 3, obtaining the quintic polynomial $p_3^*(x)$. Since $p_3(x)$ is irreducible it follows that $p_3^*(x)$ is also irreducible. We can now apply Lemma 4.2 with $D = Z, F = Q$, and $p = 3$ to conclude that $p(x)$ is irreducible, which gives us our family of infinitely many irreducible quintic polynomials.

For a concrete example we take $n = 2, d = 4$, and $e = 5$, which gives us $c = .05$ and $p(x) = 827392x^5 + 20480x^4 + 6553x^3 - 73728x^2 - 12800x - 6400$, which is an irreducible quintic polynomial with one real root. Through geometric constructions of our conchoids and circles for $a = -.5, b = .5$, and various values of c (as described in Baragar, [3]), we obtain that whenever $0 < c \le .69$ our quintic polynomial $p(x)$ has a unique real root.

We therefore have obtained infinitely many irreducible quintic polynomials with unique real roots, and have proved our main result.

Theorem 4.4. *There are infinitely many real numbers constructible by marked ruler and compass which are q-constructible.*
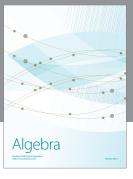

Acknowledgment

References

[1] G. E. Martin, *Geometric Constructions*, Springer, New York, NY, USA, 1998.
[2] P. Morandi, *Field and Galois Theory*, vol. 167 of *Graduate Texts in Mathematics*, Springer, New York, NY, USA, 1996.
[3] A. Baragar, "Constructions using a compass and twice-notched straightedge," *The American Mathematical Monthly*, vol. 109, no. 2, pp. 151–164, 2002.
[4] C. R. Videla, "On points constructible from conics," *The Mathematical Intelligencer*, vol. 19, no. 2, pp. 53–57, 1997.
[5] J. Robertson and C. Snyder, "A simple geometric construction involving ultraradicals," *Journal of the Australian Mathematical Society*, vol. 91, no. 1, pp. 103–124, 2011.
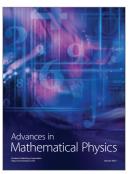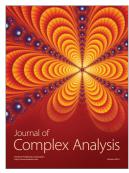[6] S. Lang, *Undergraduate Algebra*, Springer, New York, NY, USA, 2005.