Global Journal of Advanced Research
on Classical and Modern Geometries
ISSN: 2284-5569, Vol.12, (2023), Issue 1, pp.126-142

QUADRILATERAL INSCRIBED IN SEMICIRCLES THAT ARE CONSTRUCTIBLE WITH RULER AND COMPASS

MIRCEA GOTEA AND AUREL I. STAN

ABSTRACT. We describe the positive numbers a, b, and c, which belong to the field G of numbers that are constructible with a ruler and compass, such that there exists a cyclic quadrilateral $ABCD$, inscribed in a semicircle of radius R, whose lengths are $AB = a$, $BC = b$, $CD = c$, and $DA = 2R$ (the diameter of the circumscribed circle), such that the radius R is also a number constructible with a ruler and compass.

1. INTRODUCTION AND MOTIVATIONS

In this section we present the motivation and some well known results related to the paper.

Pythagoras theorem states that in a right triangle, the sum of the squares of the lengths of the legs is equal to the square of the length of the hypothenuse. In [3] and [4], the author extended this classic result to general polygons making the observation that since the measure of an angle, with the vertex on a circle, is half of the measure of the subtended arc, of that circle, a right triangle is in fact, a triangle that can be inscribed in a semicircle, that means, a triangle in which one of the sides (the longest one) is a diameter of the circumscribed circle. Starting from this observation, the author generalized Pythagoras theorem to cyclic polygons that are inscribed in a semicircle, that means cyclic polygons for which one of the sides is a diameter of the circumscribed circle. One interesting thing is the fact that, for a cyclic quadrilateral inscribed in a semicircle, the equation that relates the length of the longest side (or equivalently the radius of the circumscribed circle) to the lengths of the other sides is a cubic equation (no longer a quadratic one). This fact raises the following questions. Is it possible that if the lengths of the other three sides are numbers constructible with a ruler and compass, the length of the longest side, which is equal to the diameter of the circumscribed circle, may not be a number constructible with a ruler and compass? If so, can we describe the cyclic quadrilaterals inscribed in a semicircle for which the lengths of all the four sides are numbers constructible with a ruler and compass? The purpose of this paper is to answer these two questions.

The paper is structured as follows. In subsection 1.1, we present the equation that relates the radius (or equivalently the diameter) of the circumscribed circle to the length of the three shorter sides of a cyclic quadrilateral inscribed in a semi-circle. In subsection 1.2,

2010 *Mathematics Subject Classification.* Primary 51M15; Secondary 51M04.
Key words and phrases. Pythagoras theorem, law of cosines, numbers constructible with a ruler and compass, irreducible polynomials.

we review briefly the field of numbers constructible with a ruler and compass. Finally, in section 2, we describe all the cyclic quadrilaterals inscribed in a semicircle whose sides have lengths numbers that are constructible with a ruler and compass.

1.1. **A Pythagorean theorem for cyclic quadrilaterals inscribed in a semicircle.** This theorem is taken from [3] and [4].

Theorem 1.1. *Let $ABCD$ be a cyclic quadrilateral in which the side AD is a diameter of the circumscribed circle. Let the lengths of its sides be $AB = a$, $BC = b$, $CD = c$, and $DA = 2R$, where R denotes the radius of the circumscribed circle of the cyclic quadrilateral $ABCD$. Then we have:*

$$(2R)^3 - \left(a^2+b^2+c^2\right)(2R) - 2abc \;=\; 0. \tag{1.1}$$

Proof. Since the angle $\sphericalangle ABD$ subtends a semicircle, it is a right angle. Applying first the Pythagorean theorem in the right triangle ABD and then the Law of Cosines in the triangle BCD, we have:

$$\begin{aligned} AD^2 &= AB^2 + BD^2 \\ &= AB^2 + BC^2 + CD^2 - 2BC\cdot CD\cdot\cos(\sphericalangle BCD) \end{aligned}$$

Since the quadrilateral $ABCD$ is cyclic, we have $m(\sphericalangle BCD) = 180^\circ - m(\sphericalangle DAB)$ and since for all angles α, $\cos(180^\circ - \alpha) = -\cos(\alpha)$, we obtain:

$$\begin{aligned} AD^2 &= AB^2 + BC^2 + CD^2 - 2BC\cdot CD\cdot\cos(\sphericalangle BCD) \\ &= AB^2 + BC^2 + CD^2 + 2BC\cdot CD\cdot\cos(\sphericalangle DAB). \end{aligned}$$

Substituting $\cos(\sphericalangle DAB)$ by the ratio AB/AD (from the right triangle ABD) in the last relation, we obtain:

$$\begin{aligned} AD^2 &= AB^2 + BC^2 + CD^2 + 2BC\cdot CD\cdot\cos(\sphericalangle DAB) \\ &= AB^2 + BC^2 + CD^2 + 2BC\cdot CD\cdot\frac{AB}{AD}. \end{aligned}$$

Multiplying both sides of the last equation by AD, we obtain:

$$AD^3 \;=\; \left(AB^2+BC^2+CD^2\right)AD + 2AB\cdot BC\cdot CD,$$

which is equivalent to:

$$(2R)^3 - \left(a^2+b^2+c^2\right)(2R) - 2abc \;=\; 0.$$

□

Let us observe that the formula (1.1) is symmetric in a, b, and c, and it does not matter that the sides of lengths a and c are adjacent to the diameter side of length $2R$, while the side of length b is opposite to the diameter side DA. This can also be seen geometrically by drawing the diameter BB' (that means, B' is the point that is diametrically opposite to B in the circumscribed circle of the cyclic quadrilateral $ABCD$). We can see now, that the quadrilateral $BCDB'$ is cyclic and inscribed in a semicircle, in which the sides of lengths b and a are adjacent to the diametral side $BB' = 2R$, while the side of length c is opposite to the diametral side BB'. This confirms that in the algebraic formula (1.1), the sides of length a, b, and c are playing a symmetric role, and it does not matter which sides are adjacent to the diametral (longest) side and which side is opposite to it.

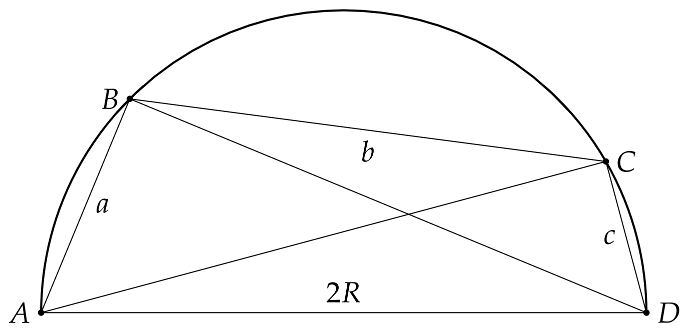

Figure 1. M1

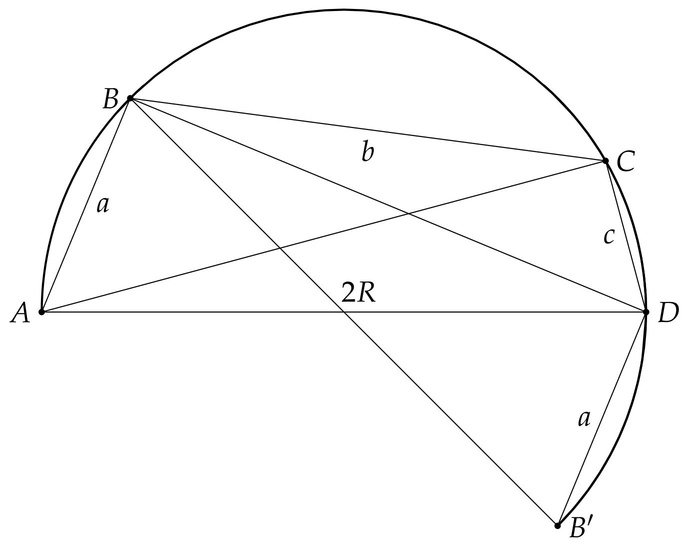

Figure 2. M2

It was also shown in [3] and [4], that if a, b, c, and R are positive numbers satisfying equation (1.1), then there exists a cyclic quadrilateral $ABCD$ inscribed in a semi-circle of radius R such that: $AB = a$, $BC = b$, $CD = c$, and $DA = 2R$.

We would like to answer now the following question:
Question 1 *Is it true that if a, b, and c are positive numbers constructible with a ruler a compass, then the radius R (or equivalently the diameter $2R$) is also constructible with a ruler and compass?*
If the answer for this question is "No", then we would like to answer the second question:
Question 2 *Can we describe all the positive numbers a, b, and c, that are constructible with a ruler a compass, for which the radius R (or equivalently the diameter $2R$) is also constructible with a ruler and compass?*
To answer these questions, we are reviewing the field of the numbers constructible with a ruler and compass in the next subsection.

1.2. **The field of numbers constructible with a ruler and compass.** In this subsection, we review briefly the field of numbers constructible with a ruler and compass.
Every construction with a ruler and compass starts from a given set S_0 of at least two points, $\{(x_{0,j}, y_{0,j})\}_{j\in J}$, in the plane, that are identified with the complex numbers $\{z_{0,j} = x_{0,j} + iy_{0,j}\}_{j\in J}$, and drawing all possible lines joining two of these points and all circles centered at one of these points of radius equal to the distance between any two of these points, we create a new set S_1 of points that are at the intersection of two lines, or a line and a circle, or two circles from the lines and circles described above. We can see that $S_0 \subseteq S_1$. Then we repeat the procedure with the new set of points S_1 replacing the set of points S_0, obtaining a larger set S_2 (that means, $S_0 \subseteq S_1 \subseteq S_2$), and so on. Continuing this construction indefinitely, we obtain a sequence of increasing sets:

$$S_0 \subseteq S_1 \subseteq S_2 \subseteq \cdots . \tag{1.2}$$

The union of all these sets:

$$S \;:=\; \cup_{n=0}^{\infty} S_n \tag{1.3}$$

is called the *set of points constructible with a ruler and compass from the set S_0*.
Now, let us suppose that at the stage n of our construction, when the set S_n has been constructed, and we are ready to construct the new larger set S_{n+1}, we know that S_n (in which each point has been identified with its corresponding complex number) is contained in a certain subfield F of the field of complex numbers $\mathbb{C}$. Then a point z in the new set S_{n+1} is constructed in one of the following three ways:

- z is the intersection of a line l_1, joining the points z_1 and z_2 from S_n, and another line l_2 joining the points z_3 and z_4 from S_n. Since z_1, z_2, z_3, and z_4 are all in the field F, and finding the intersection of two lines requires to solve a linear system of two equations, we can easily see that the point z remains in the field F.
- z is the intersection of a line l, joining the points z_1 and z_2 from S_n, and a circle $\mathcal{C}$ centered at a point z_3 from S_n, and of radius $|z_4 - z_5|$, with z_4 and z_5 in S_n. Since finding the intersection of a line and a circle, in Analytic Geometry, reduces in the end to solving a quadratic equation, we can see that z is a root of a quadratic equation with coefficients in the field F. Thus z is algebraic over the field F and the degree of the extension of fields $F \subseteq F(\alpha)$, where $F(\alpha)$ denotes the smallest field containing $F \cup \{\alpha\}$, is:
$$[F(\alpha) : F] \;=\; 2^{\epsilon}, \tag{1.4}$$
with $\epsilon \in \{0, 1\}$.
- z is the intersection of a circle $\mathcal{C}_1$, centered at a point z_1 from S_n and of radius $|z_2 - z_3|$, for some z_2 and z_3 in S_n, and another circle $\mathcal{C}_2$, centered at a point z_4 from S_n, and of radius $|z_5 - z_6|$, for some z_5 and z_6 in S_n. Since finding the intersection of two circles means to solve a system of two quadratic equations in x and y, in which the coefficients of x^2 and of y^2 in both equations are equal to 1, which by subtracting the two equations is equivalent to solving a system consisting of a linear equation (the equation of the radical axis of the two circles) and a quadratic equation (the equation of anyone of the two circles), this case can be reduced to the previous case. Thus z is algebraic over the field F and the degree of the extension of fields $F \subseteq F(\alpha)$ is:
$$[F(\alpha) : F] \;=\; 2^{\epsilon}, \tag{1.5}$$

with $\epsilon \in \{0, 1\}$.

Because solving a quadratic equation by the quadratic formula involves the computation of the radical of its discriminant, we can see that somehow the set of numbers constructible with a ruler and compass, from a given set of points, requires a constant (continuous) enrichment of the set with the radicals of the existing (already constructed) numbers.

In the classic field of numbers constructible with a ruler and compass, the starting set S_0 is the set formed by only two points (0, 0), identified with the complex number $0 = 0 + 0i$, and the point (1, 0), identified with the complex number $1 = 1 + 1i$. One can easily see that starting with this set $S_0 = \{0, 1\} \subset \mathbb{C}$ is equivalent to starting with $G_0 = \mathbb{Q}$, where $\mathbb{Q}$ denotes the field of the rational numbers, since the rational numbers can be easily constructed from the points of affixes 0 and 1 by a ruler and compass.

Then we construct the field G_1 as the smallest field containing the rational numbers $\mathbb{Q}$ and all the radicals of rational numbers, that means all the complex numbers α for which $\alpha^2 \in \mathbb{Q}$. A precise mathematical description of this field is:

$$G_1 = \left\{c_1 \cdot \alpha_1 + c_2 \cdot \alpha_2 + \cdots + c_n \cdot \alpha_n \mid n \in \mathbb{N}, \forall 1 \le i \le n, c_i \in \mathbb{Q}, \alpha_i \in \mathbb{C}, \alpha_i^2 \in \mathbb{Q}\right\}.$$

It is easy to check that G_1 satisfies all the properties of a field, but the property that every non-zero element of G_1 has an inverse, that is also an element of G_1, is not so obvious. We are checking this property below.

Indeed, let

$$x = c_1 \cdot \alpha_1 + c_2 \cdot \alpha_2 + \cdots + c_n \cdot \alpha_n \in G_1, \tag{1.6}$$

such that $x \neq 0$, where we have chosen n to be the smallest possible natural number for which the decomposition (1.6) of x holds. Due to the minimality of n, the numbers α_1, $\alpha_2, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$. Let us define now the following set:

$$Con_x = \{\epsilon_1 c_1 \cdot \alpha_1 + \epsilon_2 c_2 \cdot \alpha_2 + \cdots + \epsilon_n c_n \cdot \alpha_n \mid \forall 1 \le i \le n, \epsilon_i \in \{-1, 1\}\}. \tag{1.7}$$

Intuitively, Con_x is the set of all conjugates of x and $-x$.

Then Con_x has 2^n elements, all of them being elements of G_1 different from zero (due to the fact that $\alpha_1, \alpha_2, \ldots, \alpha_n$ are linearly independent), one of them being the number x. Let us multiply all the $\mathbb{Q}$-conjugates of x and $-x$, and define the non-zero number:

$$u := \prod_{y \in Con_x} y. \tag{1.8}$$

It is clear that $u = f(\alpha_1, \alpha_2, \ldots, \alpha_n)$, where f is a polynomial of n-variables with rational coefficients. Moreover, for all $i \in \{1, 2, \ldots, n\}$, we have:

$$f(\alpha_1, \ldots, \alpha_{i-1}, -\alpha_i, \alpha_{i+1}, \ldots, \alpha_n) = f(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i, \alpha_{i+1}, \ldots, \alpha_n), \tag{1.9}$$

which shows that $f(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is made up of terms that are products of even powers of $\alpha_1, \alpha_2, \ldots, \alpha_n$. Since $\alpha_1^2 \in \mathbb{Q}$, $\alpha_2^2 \in \mathbb{Q}, \ldots, \alpha_n^2 \in \mathbb{Q}$, we conclude that $u = f(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Q} \setminus \{0\}$. Thus, we have:

$$\begin{aligned} x \cdot \frac{1}{u} \prod_{y \in Con_x, y \neq x} y &= \frac{1}{u} \cdot \prod_{y \in Con_x} y \\ &= \frac{1}{u} \cdot u \\ &= 1, \end{aligned} \tag{1.10}$$

and so, we can see that x has the inverse $(1/u)\prod_{y\in Con_x, y\neq x} y \in G_1$.
Next we construct the field G_2 as the smallest field containing the numbers from G_1 and all the complex numbers α for which $\alpha^2 \in G_1$, and so on. In general having constructed the field G_n, the field G_{n+1} is the smallest field containing G_n and all complex numbers α such that $\alpha^2 \in G_n$. The set of numbers constructible with a ruler and compass form a field and is equal to the set:

$$G \;:=\; \cup_{n=0}^{\infty} G_n. \tag{1.11}$$

Another characterization of the field of the numbers constructible with a ruler and compass is the following:

Theorem 1.2. *The set of numbers constructible with a ruler and compass is the smallest normal extension of the field of rational numbers* $\mathbb{Q}$ *that is closed with respect to taking radicals (square roots).*

From the above construction it follows easily the following corollary:

Corollary 1.1. *If* α *is a complex number constructible with a ruler and compass, then* α *is an algebraic number, and the degree of its minimal polynomial over the field of rational numbers,* $\mathbb{Q}$*, is a perfect power of* 2.

2. MAIN RESULTS

In this section we present the main results related to the paper. More precisely, we give a description of all positive numbers a, b, and c, that are constructible with a ruler and compass, such that the positive solution $2R$ of equation (1.1) is also a number constructible with a ruler and compass. Before doing this, we establish first the following result:

Proposition 2.1. *For all positive numbers* a, b, *and* c, *the cubic equation:*

$$x^3 - \left(a^2 + b^2 + c^2\right)x - 2abc \;=\; 0 \tag{2.1}$$

has three real solutions out of which one is positive and two are negative (with the possibility of the negative roots being equal). Moreover, the positive root is located in the interval $(\max\{a, b, c\}, a + b + c)$.

Proof. Indeed, let us define the cubic function:

$$f(x) \;=\; x^3 - \left(a^2 + b^2 + c^2\right)x - 2abc. \tag{2.2}$$

Its derivative:

$$f'(x) \;=\; 3x^2 - \left(a^2 + b^2 + c^2\right) \tag{2.3}$$

has two distinct real solutions $x_1 < 0 < x_2$, where:

$$x_1 \;=\; -\sqrt{\frac{a^2 + b^2 + c^2}{3}} \tag{2.4}$$

and

$$x_2 \;=\; \sqrt{\frac{a^2 + b^2 + c^2}{3}}. \tag{2.5}$$

We have:

$$\begin{aligned} f(-\infty) &= \lim_{x\to-\infty}\left[x^3-\left(a^2+b^2+c^2\right)x-2abc\right] \\ &= -\infty. \end{aligned} \tag{2.6}$$

On the other hand, using the arithmetic-geometric mean inequality

$$\begin{aligned} f(x_1) &= -\frac{1}{3\sqrt{3}}\left(a^2+b^2+c^2\right)^{3/2}+\frac{1}{\sqrt{3}}\left(a^2+b^2+c^2\right)^{3/2}-2abc \\ &= 2\left[\left(\frac{a^2+b^2+c^2}{3}\right)^{3/2}-abc\right] \qquad (2.7) \\ &\geq 0. \qquad (2.8) \end{aligned}$$

If a, b, and c are not all three equal, then the inequality between the arithmetic and geometric means of a^2, b^2, and c^2 is strict, and so $f(x_1) > 0$.
If $a = b = c$, then $x_1 = -a = -b = -c$, and so, we have $f(x_1) = f'(x_1) = 0$, which means that x_1 is a double negative root.
We also have:

$$\begin{aligned} f(0) &= -2abc \qquad (2.9) \\ &< 0, \qquad (2.10) \end{aligned}$$

and

$$\begin{aligned} f(\infty) &= \lim_{x\to\infty}\left[x^3-\left(a^2+b^2+c^2\right)x-2abc\right] \\ &= \infty. \end{aligned} \tag{2.11}$$

Thus, we can see that:

- If a and b and c are not all three equal, then f changes its sign from one end to the other on each of the three intervals: $(-\infty, x_1)$, $(x_1, 0)$, and $(0, \infty)$, and since f is a continuous function (being polynomial), f has three distinct roots: one in $(-\infty, x_1)$, one in $(x_1, 0)$, and one in $(0, \infty)$, by the Darboux property.
- If $a = b = c$, then f has a repeated (double) negative root $x = x_1$ and a root in $(0, \infty)$.

Let us show now that the positive root of f is located in the interval $(\max\{a, b, c\}, a+b+c)$.
Indeed, assuming that $\max\{a, b, c\} = a$, we have:

$$\begin{aligned} f(a) &= a^3-\left(a^2+b^2+c^2\right)a-2abc \\ &= -a(b+c)^2 \\ &< 0 \end{aligned} \tag{2.12}$$

and

$$\begin{aligned} f(a+b+c) &= (a+b+c)\left[(a+b+c)^2-\left(a^2+b^2+c^2\right)\right]-2abc \\ &= (a+b+c)(2ab+2bc+2ca)-2abc \\ &> a(2bc)-2abc \\ &= 0. \end{aligned} \tag{2.13}$$

Thus, by the Darboux property, f has a root in the interval $(a, a+b+c)$. □

Now, we show that the answer to Question 1 is negative, that means, there exist a, b, and c positive numbers constructible with a ruler and compass, such that the roots of the cubic equation (2.1) are not constructible with a ruler and compass.

Example 2.1. *Let $a = 1$, $b = 2$, and $c = 5$. These are rational numbers, and so they are numbers constructible with a ruler and compass. The cubic equation (2.1) becomes:*

$$x^3 - \left(1^2 + 2^2 + 5^2\right) x - 2(1)(2)(5) = 0, \tag{2.14}$$

that means:

$$x^3 - 30x - 20 = 0. \tag{2.15}$$

Observe that the cubic polynomial $f(x) = x^3 - 30x - 20$ is irreducible since the prime number $p := 5$ satisfies:

$$5 \nmid 1, \quad 5 \mid 0, \quad 5 \mid -30, \quad 5 \mid -20, \quad \text{and} \quad 5^2 \nmid -20. \tag{2.16}$$

Thus, by Eisenstein irreducibility criterion, $f(x)$ is an irreducible polynomial over $\mathbb{Q}$. Hence, it is the minimal polynomial of the diameter $2R$ of the circumscribed semicircle. Therefore, $2R$ (and also R) is not constructible with a ruler and compass since the degree of the extension $[\mathbb{Q}(R) : \mathbb{Q}] = 3$ which is not a perfect power of 2.

We are now going to describe all positive numbers a, b, and c, that are constructible with a ruler and compass, for which the diameter $2R$ of the circumscribed semicircle is constructible with a ruler and compass. Since $2R$ is the positive solution of the cubic polynomial $f(X) = X^3 - (a^2 + b^2 + c^2)X - 2abc$, which has coefficients in the field G of the numbers constructible with a ruler and compass, $2R$ is constructible with a ruler and compass if and only if this polynomial is not irreducible in the ring of polynomials $G[X]$. Indeed, if $f(X)$ is not irreducible in $G[X]$, then since it has degree 3, it factorizes as product of one polynomial $g(X)$, of degree 1, in $G[X]$, and another polynomial $h(X)$ of degree 2, in $G[X]$. That means:

$$f(X) = (X - \alpha)\left(X^2 - \beta X + \gamma\right), \tag{2.17}$$

with α, β, and γ in G. Then either $2R = \alpha \in G$, or $2R$ is a root of the polynomial $h(X) = X^2 - \beta X + \gamma$, which means:

$$2R = \frac{\beta \pm \sqrt{\beta^2 - 4\gamma}}{2} \tag{2.18}$$

$$\in G, \tag{2.19}$$

since the field G of numbers constructible with a ruler and compass is closed with respect to taking radicals. In this case, we can see that $2R$ is constructible with a ruler and compass.

On the other hand, if $f(X)$ is irreducible in $G[X]$, then since $f(X) \in \mathbb{Q}(a, b, c)[X] \subset G[X]$, $f(X)$ is also irreducible over $\mathbb{Q}(a, b, c)[X]$, and because $2R$ is a root of this polynomial, $f(X)$ is the minimal polynomial of $2R$ over $\mathbb{Q}(a, b, c)$. Thus, we have $[\mathbb{Q}(a, b, c, 2R) : \mathbb{Q}(a, b, c)] = 3$. That means,

$$\begin{aligned} [\mathbb{Q}(a,b,c,2R) : \mathbb{Q}] &= [\mathbb{Q}(a,b,c,2R) : \mathbb{Q}(a,b,c)] \cdot [\mathbb{Q}(a,b,c) : Q] \\ &= 3 \cdot [\mathbb{Q}(a,b,c) : Q]. \end{aligned} \tag{2.20}$$

That means, $[\mathbb{Q}(a, b, c, 2R) : \mathbb{Q}]$ is not a perfect power of 2. Therefore, one of the four numbers a, b, c, and $2R$ is not constructible with a ruler and compass, and since a, b, and c are assumed to be constructible with a ruler and compass, we conclude that $2R$ is not constructible with a ruler and compass. Before proving the main result of this paper, we make one more remark:

Remark 2.1. *If a, b, and c are numbers in a field F, where $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$, such that the polynomial $f_{a,b,c}(X) := X^3 - \left(a^2 + b^2 + c^2\right) X - 2abc$ is not irreducible in the ring of polynomials $F[X]$, then for all ϵ_1, ϵ_2, and ϵ_3 in $\{-1, 1\}$, the polynomial $f_{a',b',c'}(X) := X^3 - \left(a'^2 + b'^2 + c'^2\right) X - 2a'b'c'$ is also not irreducible in $F[X]$, where $a' := \epsilon_1 a$, $b' := \epsilon_2 b$, and $c' := \epsilon_3 c$.*

Proof. Indeed, since $a' = \pm a$, $b' = \pm b$, $c' = \pm c$, we have:

$$a'^2 + b'^2 + c'^2 = a^2 + b^2 + c^2 \tag{2.21}$$

and

$$2a'b'c' = \pm 2abc. \tag{2.22}$$

We have two cases:
Case 1: If $a'b'c' = abc$, then $f_{a',b',c'}(X) = f_{a,b,c}(X)$ and we are done.
Case 2: If $a'b'c' = -abc$, then:

$$\begin{aligned} f_{a',b',c'}(X) &= X^3 - \left(a'^2 + b'^2 + c'^2\right) X - 2a'b'c' \\ &= X^3 - \left(a^2 + b^2 + c^2\right) X + 2abc \\ &= -\left[(-X)^3 - \left(a^2 + b^2 + c^2\right)(-X) - 2abc\right] \\ &= -f_{a,b,c}(-X). \end{aligned} \tag{2.23}$$

From here, it follows clearly that if $f_{a,b,c}(X)$ is not irreducible in $F[X]$, then $f_{a',b',c'}(X)$ is not irreducible in $F[X]$, too. □

Theorem 2.1. *A cyclic quadrilateral $ABCD$ inscribed in a semicircle of radius R has all four sides $AB = a$, $BC = b$, $CD = c$, and $DA = 2R$ numbers that are constructible with a ruler and compass if and only if there exist three real numbers λ, m, and p, that are constructible with a ruler and compass, such that:*

$$a = \left|\left(m^2 - \lambda\right)\left(p^2 + \lambda\right)\right|, \tag{2.24}$$

$$b = \left|\left(m^2 - \lambda\right)\left(p^2 - \lambda\right) \pm 4\lambda mp\right|, \tag{2.25}$$

and

$$c = \left|\left(m^2 + \lambda\right)\left(p^2 - \lambda\right)\right|, \tag{2.26}$$

with the assumption that none of the three numbers inside the absolute value in the above expressions is equal to 0.

Proof. $(\Rightarrow)$ Let us assume that there exist three real numbers λ, m, and p, constructible with a ruler and compass, such that formulas (2.24), (2.25), and (2.26) hold. Since the set of numbers constructible with a ruler and compass form a field, it follows that a, b, and c are constructible with a ruler and compass. It remains to show that the diameter $2R$ of the circumscribed semicircle is also constructible with a ruler and compass. For this, we have to show that the cubic polynomial $f_{a,b,c}(X) = X^3 - (a^2 + b^2 + c^2)X - 2abc$ is not irreducible in the ring of polynomials $G[X]$, where G denotes the field of numbers constructible with a ruler and compass. According to Remark 2.1, $f_{a,b,c}$ is not irreducible in $G[X]$ if and only if $f_{\pm a,\pm b,\pm c}$ is not irreducible in $G[X]$. So, we can ignore the absolute values from the definitions of a, b, c, and show that $f_{a',b',c'}$ is not irreducible in $G[X]$, where:

$$a' := \left(m^2-\lambda\right)\left(p^2+\lambda\right), \tag{2.27}$$

$$b' := -\left(m^2-\lambda\right)\left(p^2-\lambda\right) \pm 4\lambda mp, \tag{2.28}$$

and

$$c' := \left(m^2+\lambda\right)\left(p^2-\lambda\right). \tag{2.29}$$

Claim: $f_{a',b',c'}(x_0) = 0$, where:

$$x_0 := \left(m^2+\lambda\right)\left(p^2+\lambda\right). \tag{2.30}$$

Indeed, we have:

$$\begin{aligned} & f_{a',b',c'}\left(x_0\right) \\ = \;& x_0\left(x_0^2-a'^2-b'^2-c'^2\right)-2a'c'b' \\ = \;& \left(m^2+\lambda\right)\left(p^2+\lambda\right)\left(x_0^2-a'^2-b'^2-c'^2\right)-2\left(m^2-\lambda\right)\left(p^2+\lambda\right)\left(m^2+\lambda\right)\left(p^2-\lambda\right)b' \\ = \;& \left(m^2+\lambda\right)\left(p^2+\lambda\right)\left[x_0^2-a'^2-c'^2-b'^2-2\left(p^2-\lambda\right)\left(m^2-\lambda\right)b'\right]. \end{aligned}$$

To show that $f_{a',b',c'}(x_0) = 0$, we will prove that:

$$x_0^2-a'^2-c'^2-b'^2-2\left(p^2-\lambda\right)\left(m^2-\lambda\right)b' = 0. \tag{2.31}$$

Indeed, we have:

$$\begin{aligned} & x_0^2-a'^2-c'^2-b'^2-2\left(p^2-\lambda\right)\left(m^2-\lambda\right)b' \\ = \;& x_0^2-a'^2-c'^2-b'\left[b'+2\left(p^2-\lambda\right)\left(m^2-\lambda\right)\right] \\ = \;& x_0^2-a'^2-c'^2-b'\left[\pm4\lambda mp-\left(p^2-\lambda\right)\left(m^2-\lambda\right)+2\left(p^2-\lambda\right)\left(m^2-\lambda\right)\right] \\ = \;& x_0^2-a'^2-c'^2 \\ & -\left[\pm4\lambda mp-\left(p^2-\lambda\right)\left(m^2-\lambda\right)\right]\left[\pm4\lambda mp+\left(p^2-\lambda\right)\left(m^2-\lambda\right)\right]. \end{aligned}$$

Using now the difference of two squares formula, we obtain:

$$\begin{aligned} & x_0^2-a'^2-c'^2-b'^2-2\left(p^2-\lambda\right)\left(m^2-\lambda\right)b' \\ = \;& \left(m^2+\lambda\right)^2\left(p^2+\lambda\right)^2-\left(m^2-\lambda\right)^2\left(p^2+\lambda\right)^2-\left(m^2+\lambda\right)^2\left(p^2-\lambda\right)^2 \\ & -\left[16\lambda^2m^2p^2-\left(m^2-\lambda\right)^2\left(p^2-\lambda\right)^2\right] \\ = \;& \left(m^2+\lambda\right)^2\left(p^2+\lambda\right)^2-\left(m^2-\lambda\right)^2\left(p^2+\lambda\right)^2-\left(m^2+\lambda\right)^2\left(p^2-\lambda\right)^2 \\ & +\left(m^2-\lambda\right)^2\left(p^2-\lambda\right)^2-16\lambda^2m^2p^2 \\ = \;& \left[\left(m^2+\lambda\right)^2-\left(m^2-\lambda\right)^2\right]\left[\left(p^2+\lambda\right)^2-\left(p^2-\lambda\right)^2\right]-16\lambda^2m^2p^2 \\ = \;& \left(4m^2\lambda\right)\cdot\left(4p^2\lambda\right)-16\lambda^2m^2p^2 \\ = \;& 0. \end{aligned}$$

Thus, $f_{a',b',c'}$ has a root $x_0 \in G$. Therefore, $f_{a',b',c'}$ is not irreducible over the field G of numbers constructible with a ruler and compass.

($\Leftarrow$). Let us assume now that a, b, and c are positive numbers constructible with a ruler and compass, such that the radius R of the circumscribed semicircle is also constructible with a ruler and compass.
Since a, b, and c are constructible with a ruler and compass, and the field G of the numbers constructible with a ruler and compass is the union of the increasing sequence of fields G_n, $n \geq 0$, described in the previous section, there exists a non-negative integer n_0, such that $a \in G_{n_0}$, $b \in G_{n_0}$, and $c \in G_{n_0}$. Then the polynomial $f(X) = X^3 - \left(a^2+b^2+c^2\right)X - 2abc$ belongs to the ring of polynomials $G_{n_0}[X]$, and since $2R$ is a root of this polynomial, we have seen that $2R$ is a number constructible with a ruler and compass if and only if this polynomial is reducible in $G_{n_0}[X]$. Because f has degree 3, in order to be reducible, it must be factored as a product of a one degree polynomial and a second degree polynomial with coefficients in G_{n_0}. Due to the one degree factor, f must have a root x_0 in G_{n_0}. Thus, there exists $x_0 \in G_{n_0}$, such that $f(x_0) = 0$. This means,

$$x_0^3 - \left(a^2+b^2+c^2\right)x_0 - 2abc = 0. \tag{2.32}$$

Multiplying both sides of this equation by (-1) and re-arranging it as an equation in b, we have:

$$x_0 b^2 + (2ac)b + x_0\left(a^2+c^2-x_0^2\right) = 0. \tag{2.33}$$

This is a quadratic equation in b, with coefficients in G_{n_0}. Applying the quadratic formula, we can solve it for b, as:

$$b = \frac{-ac \pm \sqrt{a^2c^2 - a^2x_0^2 - c^2x_0^2 + x_0^4}}{x_0}, \tag{2.34}$$

which is equivalent to:

$$b = \frac{-ac \pm \sqrt{\left(x_0^2-a^2\right)\left(x_0^2-c^2\right)}}{x_0}. \tag{2.35}$$

We would like to make a comment, and observe that formula (2.35), in the case when $x_0 = 2R$ is nothing but the Ptolemy theorem, which says that in a cyclic quadrilateral, the sum of the products of the opposite sides is equal to the product of the diagonals. Anyway, in equation (2.35), x_0 is not necessarily equal to $2R$, but it represents a root of the cubic polynomial $f(X)$ that must be in G_{n_0}, in order for this polynomial to not be irreducible in $G_{n_0}[X]$. Since $b \in G_{n_0}$, the discriminant $(x_0^2-a^2)(x_0^2-c^2)$ that appears under the radical in formula (2.35) must be the square of a number from G_{n_0}. That means, there exists $k \in G_{n_0}$ such that:

$$\left(x_0^2-a^2\right)\left(x_0^2-c^2\right) = k^2. \tag{2.36}$$

This equation implies that there exist λ, u, and v in G_{n_0}, such that $\lambda \neq 0$ and:

$$\begin{cases} x_0^2 - a^2 = \lambda u^2 \\ x_0^2 - c^2 = \lambda v^2 \\ k = \lambda uv \end{cases}. \tag{2.37}$$

Indeed, if $k \neq 0$, then one may take $\lambda := x_0^2 - a^2 \neq 0$, $u := 1$, and $v := k/(x_0^2 - a^2)$.
If $k = 0$, then either $x_0^2 - a^2 = 0$ and $x_0^2 - c^2 \neq 0$, in which case, one may take $u := 0$, $v := 1$, and $\lambda := x_0^2 - c^2 \neq 0$, or $x_0^2 - c^2 = 0$ and $x_0^2 - a^2 \neq 0$, in which case, one may take $v := 0$, $u := 1$, and $\lambda := x_0^2 - a^2 \neq 0$, or $x_0^2 - a^2 = x_0^2 - c^2 = 0$, in which case we may

take $u = v := 0$ and an arbitrary $\lambda \neq 0$.
We are now going to solve the system (2.37).
We have three cases:
Case 1: If $u = 0$, then the first equation of the system (2.37) implies $x_0 = \pm a$. Since x_0 is a root of $f(X)$, we have:

$$\begin{aligned} 0 &= f(\pm a) \\ &= \pm a^3 \mp \left(a^2 + b^2 + c^2\right) a - 2abc \\ &= \mp a(b \pm c)^2. \end{aligned} \tag{2.38}$$

Since $a > 0$ and $b + c > 0$, the last equation implies $x_0 = -a$ and $b - c = 0$, which means $b = c$.
Indeed, for $b = c$, the cubic equation $f(x) = 0$ becomes:

$$x^3 - \left(a^2 + 2b^2\right) x - 2ab^2 = 0 \tag{2.39}$$

which is equivalent to:

$$x(x + a)(x - a) - 2b^2(x + a) = 0, \tag{2.40}$$

that means:

$$(x + a)\left(x^2 - ax - 2b^2\right) = 0. \tag{2.41}$$

The diameter of the circumscribed semicircle is equal to the only positive root of this equation, which means:

$$2R = \frac{a + \sqrt{a^2 + 8b^2}}{2}, \tag{2.42}$$

which is clearly constructible with a ruler and compass since both a and b are constructible with a ruler and compass, and the field of numbers constructible with a ruler and compass is closed with respect to taking radicals (where by radicals, we understand square roots).
Case 2: If $v = 0$, then similarly to the previous case, we can see that $x_0 = -c$ and $b = a$. In this case,

$$2R = \frac{c + \sqrt{c^2 + 8b^2}}{2} \tag{2.43}$$

is constructible with a ruler and compass.
Case 3: If $u \neq 0$ and $v \neq 0$, then dividing the first equation of the system (2.37) by u^2, and the second equation by v^2, and factoring by the difference of two squares formula, we obtain:

$$\begin{cases} \left(\frac{x_0}{u} + \frac{a}{u}\right)\left(\frac{x_0}{u} - \frac{a}{u}\right) = \lambda \\ \left(\frac{x_0}{v} + \frac{c}{u}\right)\left(\frac{x_0}{v} - \frac{c}{v}\right) = \lambda \\ k = \lambda uv \end{cases} . \tag{2.44}$$

We can introduce new variables:

$$\begin{cases} \dfrac{x_0}{u} + \dfrac{a}{u} & =: & m \in G_{n_0} \\ \dfrac{x_0}{u} - \dfrac{a}{u} & =: & n \in G_{n_0} \\ \dfrac{x_0}{v} + \dfrac{c}{v} & =: & p \in G_{n_0} \\ \dfrac{x_0}{v} - \dfrac{c}{v} & =: & q \in G_{n_0} \\ mn = pq & = & \lambda \\ k & = & \lambda uv \end{cases} . \tag{2.45}$$

From the first two equations of the system (2.45), we obtain:

$$x_0 = \frac{u(m+n)}{2}, \tag{2.46}$$

$$a = \frac{u(m-n)}{2}, \tag{2.47}$$

and from the third and fourth equations, we get:

$$x_0 = \frac{v(p+q)}{2}, \tag{2.48}$$

$$c = \frac{v(p-q)}{2}. \tag{2.49}$$

From equations (2.46) and (2.48), it follows that:

$$u(m+n) = v(p+q). \tag{2.50}$$

Since $f(0) = -2abc \neq 0$ and $f(x_0) = 0$, we must have $x_0 \neq 0$ and so $m+n \neq 0$ and $p+q \neq 0$. Also, since $a \neq 0$ and $c \neq 0$, we must have $m-n \neq 0$ and $p-q \neq 0$. Equation (2.50) can be re-written as:

$$\frac{u}{p+q} = \frac{v}{m+n}. \tag{2.51}$$

Let us define the number:

$$t := \frac{u}{p+q} = \frac{v}{m+n} \in G_{n_0} \setminus \{0\}. \tag{2.52}$$

Then, we obtain:

$$u = t(p+q), \tag{2.53}$$

$$v = t(m+n), \tag{2.54}$$

and from equations (2.47) and (2.49), we conclude that:

$$a = \frac{t}{2}(p+q)(m-n) \tag{2.55}$$

and

$$c \;=\; \frac{t}{2}(m+n)(p-q). \tag{2.56}$$

Since $x_0 = (v/2)(p+q)$, we also obtain:

$$x_0 \;=\; \frac{t}{2}(m+n)(p+q). \tag{2.57}$$

Since $0 \neq \lambda = mn = pq$, we have $n = \lambda/m$ and $q = \lambda/p$, and substituting into formulas (2.55), (2.56), and (2.57), we obtain:

$$a \;=\; s\left(p^2+\lambda\right)\left(m^2-\lambda\right), \tag{2.58}$$

$$c \;=\; s\left(m^2+\lambda\right)\left(p^2-\lambda\right), \tag{2.59}$$

and

$$x_0 \;=\; s\left(m^2+\lambda\right)\left(p^2+\lambda\right), \tag{2.60}$$

where

$$s \;:=\; \frac{t}{2mp} \in G_{n_0} \setminus \{0\}. \tag{2.61}$$

Observe that, we have:

$$ac \;=\; s^2\left(p^4-\lambda^2\right)\left(m^4-\lambda^2\right). \tag{2.62}$$

Let us find b now. Using equations (2.35) and (2.36), we have:

$$\begin{aligned}
b &= \frac{-ac \pm \sqrt{\left(x_0^2-a^2\right)\left(x_0^2-c^2\right)}}{x_0} \\
&= \frac{-ac \pm k}{x_0} \\
&= -\frac{ac}{x_0} \pm \frac{k}{x_0} \\
&= -\frac{s^2\left(p^4-\lambda^2\right)\left(m^4-\lambda^2\right)}{s\left(m^2+\lambda\right)\left(p^2+\lambda\right)} \pm \frac{\lambda uv}{s\left(m^2+\lambda\right)\left(p^2+\lambda\right)} \\
&= -s\left(m^2-\lambda\right)\left(p^2-\lambda\right) \pm \frac{\lambda t(p+q)t(m+n)}{(t/2)(m+n)(p+q)} \\
&= -s\left(m^2-\lambda\right)\left(p^2-\lambda\right) \pm 2t\lambda \\
&= -s\left(m^2-\lambda\right)\left(p^2-\lambda\right) \pm 4smp\lambda \\
&= -s\left[\left(m^2-\lambda\right)\left(p^2-\lambda\right) \mp 4\lambda mp\right].
\end{aligned} \tag{2.63}$$

Some of the numbers a, b, and c may be negative, but according to Remark 2.1, we may replace a by $\pm a$, b by $\pm b$, and c by $\pm c$, and we are guaranteed that the cubic polynomial $f(X)$, having $2R$ as one of its roots, is reducible over $G_{n_0}[X]$. Thus, it is safe to put absolute values in the formulas for a, b, and c to make them positive.
Finally let us observe that we may absorb $|s|$ into the parameters λ, m, and p as follows. Since $|s| \in G_{n_0}$, we have $\sqrt{|s|} \in G_{n_0+1}$ and $\sqrt[4]{|s|} \in G_{n_0+2}$. Thus, because

$$|a| \;=\; \left|s\left(p^2+\lambda\right)\left(m^2-\lambda\right)\right|, \tag{2.64}$$

$$|c| = \left|s\left(p^2-\lambda\right)\left(m^2+\lambda\right)\right|, \tag{2.65}$$

and

$$|b| = \left|s\left[\left(m^2-\lambda\right)\left(p^2-\lambda\right) \pm 4\lambda mp\right]\right|, \tag{2.66}$$

we may write simply:

$$|a| = \left|\left(p^2+\lambda\right)\left(m^2-\lambda\right)\right|, \tag{2.67}$$

$$|c| = \left|\left(p^2-\lambda\right)\left(m^2+\lambda\right)\right|, \tag{2.68}$$

and

$$|b| = \left|\left[\left(m^2-\lambda\right)\left(p^2-\lambda\right) \pm 4\lambda mp\right]\right|, \tag{2.69}$$

by replacing p by $p\sqrt[4]{|s|}$, q by $q\sqrt[4]{|s|}$, and λ by $\lambda\sqrt{|s|}$.
By allowing either $m = 0$ or $n = 0$, we obtain $|c| = |b|$ or $|a| = |b|$, that means we can include Case 1 and Case 2 also in this general formula found in Case 3. We can also replace the $\pm$ sign, in the formula for b, by the $+$ sign, by eventually absorbing the minus sign, $-$, into m or into p.
Now, the proof is complete. □

Example 2.2. *Let* $m := \sqrt{\sqrt{17}+\sqrt{13}} \in G_2$, $p := \sqrt{\sqrt{17}-\sqrt{13}} \in G_2$, *and* $\lambda := 1 \in G_0$. *Then, we have:*

$$\begin{aligned} a &= \left|\left(m^2-\lambda\right)\left(p^2+\lambda\right)\right| \\ &= \left(\sqrt{17}+\sqrt{13}-1\right)\left(\sqrt{17}-\sqrt{13}+1\right) \\ &= 17-\left(\sqrt{13}-1\right)^2 \\ &= 3+2\sqrt{13} \end{aligned} \tag{2.70}$$

and

$$\begin{aligned} c &= \left|\left(m^2+\lambda\right)\left(p^2-\lambda\right)\right| \\ &= \left|\left(\sqrt{17}+\sqrt{13}+1\right)\left(\sqrt{17}-\sqrt{13}-1\right)\right| \\ &= \left|17-\left(\sqrt{13}+1\right)^2\right| \\ &= \left|3-2\sqrt{13}\right| \\ &= 2\sqrt{13}-3. \end{aligned} \tag{2.71}$$

For b in the $\pm$ formula, let us choose the sign $+$. Thus, we have:

$$\begin{aligned} b &= \left|\left(m^2-\lambda\right)\left(p^2-\lambda\right)+4\lambda mp\right| \\ &= \left|\left(\sqrt{17}+\sqrt{13}-1\right)\left(\sqrt{17}-\sqrt{13}-1\right)+4(1)\cdot\sqrt{\sqrt{17}+\sqrt{13}}\cdot\sqrt{\sqrt{17}-\sqrt{13}}\right| \\ &= \left(\sqrt{17}-1\right)^2-13+8 \\ &= 13-2\sqrt{17}. \end{aligned} \tag{2.72}$$

Then, the cubic equation satisfied by $2R$ *is:*

$$x^3 - \left(a^2 + b^2 + c^2\right) x - 2abc = 0 \tag{2.73}$$

which means:

$$x^3 - \left[\left(2\sqrt{13}+3\right)^2 + \left(2\sqrt{13}-3\right)^2 + \left(13-2\sqrt{17}\right)^2\right] x$$
$$-2\left(3+2\sqrt{13}\right)\left(2\sqrt{13}-3\right)\left(13-2\sqrt{17}\right)$$
$$= 0. \tag{2.74}$$

This equation is equivalent to:

$$x^3 - \left(359 - 52\sqrt{17}\right) x - 1118 + 172\sqrt{17} = 0. \tag{2.75}$$

One can check the above equation by hand or use an algebra calculator.
We know for sure that x_0 *or* $-x_0$ *is a solution of this equation, where:*

$$\begin{aligned} x_0 &= \left(m^2+\lambda\right)\left(p^2+\lambda\right) \\ &= \left(\sqrt{17}+\sqrt{13}+1\right)\left(\sqrt{17}-\sqrt{13}+1\right) \\ &= \left(\sqrt{17}+1\right)^2 - 13 \\ &= 5+2\sqrt{17}. \end{aligned} \tag{2.76}$$

Let us try first to see whether $x = x_0 = 5 + 2\sqrt{17}$ *is a solution of our cubic equation. We have:*

$$\begin{aligned} & x_0^3 - \left(359-52\sqrt{17}\right) x_0 - 1118 + 172\sqrt{17} \\ = & \left(5+2\sqrt{17}\right)^3 - \left(359-52\sqrt{17}\right)\left(5+2\sqrt{17}\right) - 1118 + 172\sqrt{17} \\ = & \ 0. \end{aligned} \tag{2.77}$$

Since $x_0 = 5 + 2\sqrt{17}$ *is a root of our cubic polynomial and* $x_0 > 0$*, due to the uniqueness of the positive root of our cubic polynomial, we must have* $2R = 5 + 2\sqrt{17} \in G_1$.
If x_0 *were not a solution of our cubic equation, then* $x = -x_0$ *would have been a solution, but because* $-x_0 < 0$*, to find* $2R$*, we should have first divided our cubic polynomial by* $x + x_0 = x + 5 + 2\sqrt{17}$*, and then find the positive root of the quadratic quotient using the quadratic formula. That positive root would have been the diameter* $2R$ *of the circumscribed circle, and* $2R$ *would have been for sure in the field* G_2.

References

[1] Anghel, N., *On the constructibility with ruler and compass of a minimum chord in a parabola*. Lib. Math., Vol. XVII (1997): 9-12.

[2] Courant, R. and Robbins, H., *What Is Mathematics?: An Elementary Approach to Ideas and Methods*, 2nd ed. Oxford, England: Oxford University Press, 1996.

[3] Gotea, M., *O extindere a teoremei lui Pitagora*. Gazeta Matematică – B 122 (4) (2017): 174–178.

[4] Gotea, M., *An Extension of Pythagoras Theorem*. arXiv:2101.10228 [math.GM].

[5] Lorenz, F., *Constructibility with Ruler and Compass*. In: *Algebra*. Universitext. Springer, New York, NY (2006). https://doi.org/10.1007/0-387-31608-6-1

[6] Pedoe, D., *Geometry A Comprehensive Course*, Dover Publications, Inc., New York, 1988.

[7] Shaw, A. A., *Applications of Complex Numbers to Geometry*. The Mathematics Teacher, Vol. 25, N. 4 (1932): 215-226.

RETIRED TEACHER OF MATHEMATICS
GURGHIU, MUREŞ COUNTY, ROMANIA.

Email address: mircea@gotea.ro

OHIO STATE UNIVERSITY AT MARION
1465 MOUNT VERNON AVENUE
MARION, OH 43302, U.S.A.
Email address: stan.7@osu.edu