On the area of a polygon inscribed in a circle

L'Enseignement Mathématique (2) 53 (2007), 127–153

ON THE AREA OF A POLYGON INSCRIBED IN A CIRCLE

by Y. MATSUMOTO, Y. MATSUTANI, M. ODA, T. SAKAI and T. SHIBUYA

ABSTRACT. We prove that if $n \geq 5$, the area of the general cyclic n-gon cannot be calculated from its side lengths, using only arithmetic operations and k-th roots. To prove this, we apply Galois theory.

1. INTRODUCTION

The area of a triangle is given by Heron's formula (before 75 A.D.) in terms of its side lengths a_1, a_2, a_3 :

$$\sqrt{s(s-a_1)(s-a_2)(s-a_3)}\,, \tag{1}$$

where $s = (a_1 + a_2 + a_3)/2$. Obviously, the area of a quadrilateral is not determined by its side lengths a_1, a_2, a_3, a_4 only, but if it is inscribed in a circle, Brahmagupta's formula (628 A.D.) gives the area:

$$\sqrt{(s-a_1)(s-a_2)(s-a_3)(s-a_4)}\,, \tag{2}$$

where $s = (a_1 + a_2 + a_3 + a_4)/2$. See [2]. Thus the area of a triangle or of a cyclic quadrilateral can be calculated from its side lengths by combining the four arithmetic operations of addition, subtraction, multiplication, and division, together with the operation of taking square roots. Here and in the sequel, a *cyclic polygon* is a convex polygon whose vertices all lie on the same circle.

The purpose of this paper is to prove

THEOREM 1. *If $n \geq 5$, there is no formula which expresses the area of the general cyclic n-gon in terms of its side lengths, using only arithmetic operations and k-th roots.*

As a consequence, if n is greater than four, there exists no formula like (1) or (2) for the area of a cyclic n-gon. We prove this theorem by applying Galois theory.

Blaschke [1] proved that the area of an n-gon with given side lengths $a_1, a_2, \dots, a_n$ attains a maximum if and only if the polygon is cyclic, and it is easy to see that the maximum value is independent of the order of $a_1, a_2, \dots, a_n$. To find an explicit formula for the area of a cyclic n-gon in terms of its side lengths would be an interesting problem.

The authors are grateful to Professor Koichi Yano; without his question about the maximum area of polygons with given side lengths, the present investigation would never have been undertaken. The authors are also grateful to the referees for their careful reading and useful comments and suggestions.

Note added on May 10th, 2006. We recently learned that V. V. Varfolomeev [6] has proved that the area of a cyclic n-gon is algebraic over the field $\mathbf{Q}(a_1, \dots, a_n)$ generated by the side lengths $a_1, \dots, a_n$, and that in another paper [7], he has studied the Galois group of the same equation as our (3) (equation (8) in [6]) over the field $\mathbf{Q}(a_1, \dots, a_5)$ of rational functions of the sides of a cyclic pentagon and has proved that it is isomorphic to the symmetric group S_7. His result, together with the Geometric Theorem in the same paper, immediately implies our Theorem 1 (at least for $n = 5$), though this theorem is not stated explicitly in [7]. The merit of the present paper would be that our approach is much more elementary than his.

2. Proof of Theorem 1 for $n = 5$

In this section, we will prove Theorem 1 for $n = 5$. The proof for $n \geq 6$ will be given in §5.

Let $ABCDE$ be a cyclic pentagon, as in Figure 1. Let a, b, c, d, e be the side lengths of the pentagon as shown in Figure 1. Let x be the length of the diagonal AC, and let S be the area of the pentagon.

LEMMA 1. *The diagonal length x satisfies a polynomial equation of degree 4 whose coefficients are rational functions (over the rational field $\mathbf{Q}$) of S, a, b, c, d, e.*

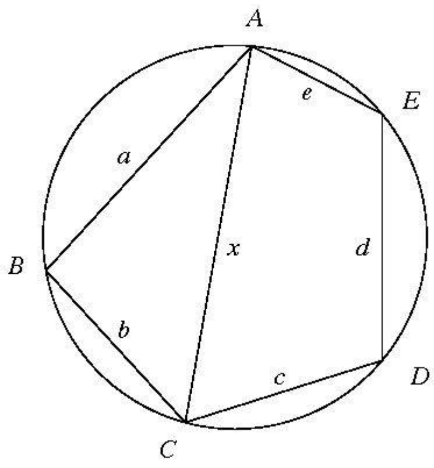

FIGURE 1
Cyclic pentagon $ABCDE$

LEMMA 2. *The diagonal length x is a solution of the following polynomial equation of degree 7:*

$$\begin{aligned}(3)\quad & cde\,x^7 + (c^2d^2 + d^2e^2 + e^2c^2 - a^2b^2)x^6 \\ & + cde\{(c^2 + d^2 + e^2) - 2(a^2 + b^2)\}x^5 \\ & + \{c^2d^2e^2 + 2a^2b^2(c^2 + d^2 + e^2) - 2(a^2 + b^2)(c^2d^2 + d^2e^2 + e^2c^2)\}x^4 \\ & + cde\{(a^2 + b^2)^2 + 4a^2b^2 - 2(a^2 + b^2)(c^2 + d^2 + e^2)\}x^3 \\ & + \{(a^2 + b^2)^2(c^2d^2 + d^2e^2 + e^2c^2) - 2c^2d^2e^2(a^2 + b^2) - a^2b^2(c^2 + d^2 + e^2)^2\}x^2 \\ & + cde(c^2 + d^2 + e^2)(a^2 - b^2)^2x + c^2d^2e^2(a^2 - b^2)^2 = 0.\end{aligned}$$

In the special case $a = b$, x is a solution of the following equation of degree 5:

$$\begin{aligned}(4)\quad & cde\,x^5 + (c^2d^2 + d^2e^2 + e^2c^2 - a^4)x^4 + cde\{(c^2 + d^2 + e^2) - 4a^2\}x^3 \\ & + \{c^2d^2e^2 + 2a^4(c^2 + d^2 + e^2) - 4a^2(c^2d^2 + d^2e^2 + e^2c^2)\}x^2 \\ & + 4a^2cde\{2a^2 - (c^2 + d^2 + e^2)\}x \\ & + a^2\{4a^2(c^2d^2 + d^2e^2 + e^2c^2) - 4c^2d^2e^2 - a^2(c^2 + d^2 + e^2)^2\} = 0.\end{aligned}$$

Let us consider for example a cyclic pentagon with side lengths $a = b = 1$, $c = 2$, $d = 3$, $e = 4$. (Such a cyclic pentagon exists. See Appendix A, Proposition 4.) Then equation (4) becomes

$$24x^5 + 243x^4 + 600x^3 - 342x^2 - 2592x - 2169 = 0.$$

Dividing out the common factor 3, we obtain

$$8x^5 + 81x^4 + 200x^3 - 114x^2 - 864x - 723 = 0\,. \tag{5}$$

LEMMA 3. *The Galois group of equation (5) over* $\mathbf{Q}$ *is* S_5, *the symmetric group of degree 5. In particular, no root of this equation belongs to radical extensions of* $\mathbf{Q}$.

Proof of Theorem 1 for $n = 5$. We will prove Theorem 1 for $n = 5$, taking Lemmas 1, 2, 3 momentarily for granted. Suppose that the area S could be calculated from the side lengths a, b, c, d, e using only arithmetic operations and k-th roots. Then by Lemma 1, x could also be calculated likewise from the side lengths, because any polynomial equation of degree 4 can be solved by radicals. This would imply that the diagonal x is in a radical extension of the field $\mathbf{Q}(a, b, c, d, e)$. In particular, equation (5) could be solved by radicals. However, this contradicts Lemma 3. Therefore, Theorem 1 is proved for $n = 5$. □

3. PROOFS OF LEMMAS 1 AND 2

Proof of Lemma 1. The area S of the cyclic pentagon $ABCDE$ of Figure 1 is the sum of the areas of the triangle ABC and the cyclic quadrilateral $ACDE$. Applying formulas (1) and (2), we have

$$\begin{aligned} S &= area(\triangle ABC) + area(\square ACDE) \\ &= \frac{1}{4}\sqrt{\{(a+b)^2 - x^2\}\{x^2 - (a-b)^2\}} \\ &\quad + \frac{1}{4}\sqrt{\{(x+c)^2 - (d-e)^2\}\{(d+e)^2 - (x-c)^2\}}\,. \end{aligned}$$

Hence,

$$\begin{aligned} &\left(4S - \sqrt{\{(a+b)^2 - x^2\}\{x^2 - (a-b)^2\}}\right)^2 \\ &= \{(x+c)^2 - (d-e)^2\}\{(d+e)^2 - (x-c)^2\}\,. \end{aligned}$$

From this, we have

$$\begin{aligned} &2(a^2 + b^2 - c^2 - d^2 - e^2)x^2 - 8cde\,x + 16S^2 - a^4 - b^4 + c^4 + d^4 + e^4 \\ &\quad - 2(-a^2b^2 + c^2d^2 + d^2e^2 + e^2c^2) = 8S\sqrt{-x^4 + 2(a^2+b^2)x^2 - (a^2-b^2)^2}\,. \end{aligned} \tag{6}$$

The required equation of degree 4 for x is obtained by squaring both sides of (6). □

Proof of Lemma 2. Let y denote the length of diagonal AD of the cyclic pentagon $ABCDE$ in Figure 1. Consider the quadrilateral $ABCD$, and let θ be the angle $\angle ABC$. Then $\angle ADC = \pi - \theta$.

We have

$$x^2 = a^2 + b^2 - 2ab\cos\theta = y^2 + c^2 - 2yc\cos(\pi - \theta).$$

Eliminating $\cos\theta$, we get

$$x^2 = \frac{(a^2 + b^2)cy + (c^2 + y^2)ab}{ab + cy}. \tag{7}$$

Similarly, considering the quadrilateral $ACDE$, we have

$$y^2 = \frac{(x^2 + c^2)de + (d^2 + e^2)cx}{cx + de}. \tag{8}$$

Eliminating y from (7) and (8), we obtain equation (3). □

4. Proof of Lemma 3

The following proposition is well known. For a proof, we refer the reader to [4] (Part II, Chap. 3, § 5).

PROPOSITION 1. *Let $P(x)$ be a polynomial of degree 5 with rational coefficients. Suppose that $P(x)$ is irreducible over $\mathbf{Q}$ and that the equation*

$$P(x) = 0 \tag{9}$$

has three real roots and a pair of imaginary roots. Then the Galois group of equation (9) over $\mathbf{Q}$ is isomorphic to the symmetric group S_5.

Therefore, in order to prove Lemma 3, it suffices to prove the following two lemmas.

LEMMA 4. *The polynomial on the left hand side of equation (5) is irreducible over $\mathbf{Q}$.*

LEMMA 5. *Equation (5) has three real roots and a pair of imaginary roots.*

Both lemmas can be checked instantly by appealing to "technological tools". We used *Mathematica*. Though our use was modest compared to that in [5], we found them very useful. We will give here, however, quite elementary proofs.

Proof of Lemma 4. Let $Q(x)$ denote the polynomial on the left hand side of equation (5). To simplify the polynomial, we define $R(x)$ by setting

$$R(x) = Q(x-2)\,. \tag{10}$$

Obviously, $Q(x)$ is irreducible over $\mathbf{Q}$ if and only if $R(x)$ is. We shall prove the irreducibility of $R(x)$. By calculation,

$$R(x) = 8x^5 + x^4 - 128x^3 - 10x^2 + 40x - 11\,.$$

As is well known, a polynomial with integral coefficients is irreducible over $\mathbf{Q}$ if and only if it is irreducible over $\mathbf{Z}$.

First of all, we prove

CLAIM 1. *The following factorization mod 8 is impossible:*

$$R(x) \equiv (x+m)T(x) \mod 8 \tag{11}$$

where m is an integer, and $T(x)$ is a polynomial with integral coefficients.

Here, by $f(x) \equiv g(x) \mod 8$, we mean that corresponding coefficients of (the polynomials) $f(x)$ and $g(x)$ are congruent modulo 8.

Proof. We have

$$R(x) \equiv x^4 - 2x^2 - 3 \mod 8\,. \tag{12}$$

If we had a factorization mod 8 of the form (11), then from (12) m would be an odd integer and therefore, $m^2 \equiv 1 \mod 8$. Also from (11), $R(-m) \equiv 0 \mod 8$. However, this is impossible, because

$$R(-m) \equiv (-m)^4 - 2(-m)^2 - 3 \equiv 1 - 2 - 3 \equiv 4 \mod 8\,.$$

This proves Claim 1.

Now we prove that $R(x)$ is irreducible over $\mathbf{Z}$.

CASE 1. If $R(x)$ were divisible in $\mathbf{Z}[x]$ by a linear polynomial, there would be integers a, b, c, d, e, k, l such that

$$R(x) = (ax + b)(cx^4 + dx^3 + ex^2 + kx + l).$$

By comparing coefficients on both sides:

$$\begin{aligned} x^5 &: \ ac = 8, \\ x^4 &: \ ad + bc = 1, \\ x^3 &: \ ae + bd = -128, \\ x^2 &: \ ak + be = -10, \\ x &: \ al + bk = 40, \\ x^0 &: \ bl = -11. \end{aligned}$$

We shall show that this system of six equations cannot be solved in integers. We may assume that $a > 0$. Since $ad + bc = 1$, we have $\gcd(a, c) = 1$. Since $ac = 8$, we have either $a = 8$, $c = 1$ or $a = 1$, $c = 8$. However, the latter case is excluded by Claim 1. Thus $a = 8$ and $c = 1$. Then $ad + bc = 1$ becomes $8d + b = 1$, whence $b \equiv 1 \mod 8$. Since b divides 11 and $b \equiv 1 \mod 8$, we have $b = 1$. Then from $8d + b = 1$ we have $d = 0$, and $ae + bd = -128$ gives $e = -16$. Now $ak + be = -10$ becomes $8k - 16 = -10$. This yields $k = \frac{3}{4}$, a contradiction.

CASE 2. If $R(x)$ were divisible in $\mathbf{Z}[x]$ by a quadratic polynomial, there would be integers a, b, c, d, e, k, l such that

$$R(x) = (ax^2 + bx + c)(dx^3 + ex^2 + kx + l). \tag{13}$$

By comparing coefficients on both sides:

$$\begin{aligned} x^5 &: \ ad = 8, \\ x^4 &: \ ae + bd = 1, \\ x^3 &: \ ak + be + cd = -128, \\ x^2 &: \ al + bk + ce = -10, \\ x &: \ bl + ck = 40, \\ x^0 &: \ cl = -11. \end{aligned}$$

We shall show that this system of six equations cannot be solved in integers. We may assume that $a > 0$. Since $ae + bd = 1$, we have $\gcd(a, d) = 1$. Since $ad = 8$, we have either $a = 8$, $d = 1$ or $a = 1$, $d = 8$. The former case is impossible. This is proved as follows: In this case, $ae + bd = 1$ would become $8e+b=1$, which implies $b\equiv 1 \mod 8$. Substituting $a=8$, $d=1$ and $b\equiv 1 \mod 8$ in (13), we would have

$$R(x)\equiv(x+c)(x^3+ex^2+kx+l) \mod 8\,,$$

which is excluded by Claim 1. Thus $a=8$, $d=1$ is impossible as asserted, and we have $a=1$, $d=8$.

Now the above system implies that

$$\begin{aligned}&e+8b=1\,,\\&k+be+8c=-128\,,\\&l+bk+ce=-10\,,\\&bl+ck=40\,,\\&cl=-11\,.\end{aligned}$$

Since $cl=-11$, there are four possiblities for the pair (c,l):

$$(c,l)=(1,-11),\ (-1,11),\ (11,-1),\ (-11,1)\,.$$

In each case, $c+l=10$ or $c+l=-10$.

CLAIM 2. *If* $c+l=10$, *then* $b\equiv 2 \mod 4$. *If* $c+l=-10$, *then* $b\equiv 0 \mod 4$.

Proof. Calculating mod 8, we have

$$\begin{aligned}&e\equiv 1\,,\\&k+b\equiv 0\,,\\&l+bk+c\equiv -2\,,\\&bl+ck\equiv 0\,.\end{aligned}$$

According as $c+l=10$ or $c+l=-10$, the third equation yields $bk\equiv -4$ or $bk\equiv 0$. The second equation implies that $bk\equiv -b^2$. Thus $b\equiv 2,6 \mod 8$ or $b\equiv 0,4 \mod 8$, according as $c+l=10$ or $c+l=-10$. This proves Claim 2.

Let $\psi(x)$ denote the quadratic factor x^2+bx+c in (13) with $a=1$. Substituting $x=\pm 2$ in $\psi(x)$ and $R(x)$, we have

$$\psi(-2)=4-2b+c\,,\quad \psi(2)=4+2b+c\,,$$

and

$$R(-2) = 653, \quad R(2) = -723.$$

Thus $\psi(-2) = 4-2b+c$ (resp. $\psi(2) = 4+2b+c$) must divide 653 (resp. 723). Note that 653 is a prime number. Thus

$$4 - 2b + c = 1, \ -1, \ 653, \text{ or } -653. \tag{14}$$

Also note that

$$653 \equiv 5 \mod 8.$$

We consider four cases according to the values of c and l.

CASE (i) $(c, l) = (1, -11)$.

Since $c+l = -10$, we have $b \equiv 0 \mod 4$ by Claim 2. Then $4-2b+1 \equiv 5 \mod 8$, and from (14), we have $4 - 2b + 1 = 653$. Therefore, $2b = -648$, and $\psi(2) = -643$. But 643 does not divide 723.

CASE (ii) $(c, l) = (-1, 11)$.

Since $c+l = 10$, we have $b \equiv 2 \mod 4$ by Claim 2. Then $4-2b-1 \equiv -1 \mod 8$, and from (14), we have $4 - 2b - 1 = -1$. Therefore, $2b = 4$, and $\psi(2) = 7$. But 7 does not divide 723.

CASE (iii) $(c, l) = (11, -1)$.

Since $c+l = 10$, we have $b \equiv 2 \mod 4$ by Claim 2. Then $4-2b+11 \equiv 3 \mod 8$, and from (14), we have $4 - 2b + 11 = -653$. Therefore, $2b = 668$, and $\psi(2) = 683$. But 683 does not divide 723.

CASE (iv) $(c, l) = (-11, 1)$.

Since $c+l = -10$, we have $b \equiv 0 \mod 4$ by Claim 2. Then $4-2b-11 \equiv 1 \mod 8$, and from (14), we have $4 - 2b - 11 = 1$. Therefore, $2b = -8$, and $\psi(2) = -15$. But 15 does not divide 723.

We have proved that the factorization (13) is impossible. Case 2 is done.

Now suppose that $R(x)$ were reducible over $\mathbf{Z}$. Then, since $R(x)$ is of degree 5, it would be divisible in $\mathbf{Z}[x]$ by a linear or a quadratic factor. However, both factorizations are impossible by Cases 1 and 2. This completes the proof of Lemma 4. $\square$

Proof of Lemma 5. Let $R(x)$ be the polynomial defined by (10). Since $R(x)$ has the same number of real roots as $Q(x)$, it suffices to prove that $R(x)$ has exactly 3 real roots. The derivative

$$R'(x) = 4(10x^4 + x^3 - 96x^2 - 5x + 10)$$

is a polynomial of degree 4, and

$$\lim_{x\to-\infty} R'(x) = +\infty,\ R'(-1) < 0,\ R'(0) > 0,\ R'(1) < 0,\ \lim_{x\to+\infty} R'(x) = +\infty\,,$$

Hence $R'(x)$ has only real roots, one in each of the intervals

$$(-\infty,-1),\quad (-1,0),\quad (0,1),\quad (1,+\infty)\,.$$

We now consider $R(x)$ on each of these intervals. Since

$$\lim_{x\to-\infty} R(x) = -\infty,\ R(-1) > 0,\ R(0) < 0,\ R(1) < 0,\ \lim_{x\to+\infty} R(x) = +\infty\,,$$

$R(x)$ has an odd number of roots in $(-\infty,-1)$, in $(-1,0)$ and in $(1,+\infty)$. It follows from Rolle's theorem and what we know about the roots of $R'(x)$, that $R(x)$ has exactly one root in each of these intervals. And $R(x)$ has no root in $(0,1)$, because

$$R(x) < 0 \quad \text{for} \quad 0 \le x \le 1\,.$$

Indeed, by writing

$$R(x) = 8x^3(x^2-1) + (x^4-1) - 10x^2 + 40x(1-3x^2) - 10\,,$$

we see that

$$R(x) < 40x(1-3x^2) - 10 \quad \text{for} \quad 0 \le x \le 1\,.$$

And $x(1-3x^2)$ attains its maximum on the interval $[0,1]$ at $x = \frac{1}{3}$, whence

$$R(x) < \frac{40}{3}(1-\frac{1}{3}) - 10 = \frac{80}{9} - 10 < 0 \quad \text{for} \quad 0 \le x \le 1\,.$$

This concludes the proof: the polynomial $R(x)$ has exactly 3 real roots, say x_1, x_2, x_3, which are such that $x_1 < -1 < x_2 < 0$ and $x_3 > 1$. □

5. Proof of Theorem 1 for $n \geq 6$

In §2, we proved that the area of a cyclic pentagon with side lengths $a = b = 1$, $c = 2$, $d = 3$, $e = 4$ does not belong to any radical extension of $\mathbf{Q}$. In this section, we will prove Theorem 1 for $n \geq 6$ by showing that the following assumption $(\star)$ contradicts the above fact.

Assumption $(\star)$. *For a certain integer $n \geq 6$, there exists an area formula $F(a_1, a_2, \ldots, a_n)$ which gives the area of an arbitrary cyclic n-gon in terms of the side lengths $a_1, a_2, \ldots, a_n$ using only the four arithmetic operations and k-th roots.*

In this section, we will assume $(\star)$, and n will always denote the particular integer specified in $(\star)$. Let S_0 denote the area of the cyclic pentagon with side lengths $a_1 = a_2 = 1$, $a_3 = 2$, $a_4 = 3$, $a_5 = 4$. If t is a sufficiently small positive real number, then by Proposition 4 of Appendix A, there exists a cyclic n-gon with side lengths

$$a_1 = a_2 = 1,\ a_3 = 2,\ a_4 = 3,\ a_5 = 4,\ a_6 = t,\ \ldots,\ a_n = t\,.$$

Note that the radius of the circumscribed circle may depend on t.

PROPOSITION 2.

$$\lim_{t\to+0} F(1,1,2,3,4,t,\ldots,t) = S_0\,. \tag{15}$$

Proof. In general, we will denote by $S(c_1, c_2, \ldots, c_m)$ the area of a cyclic m-gon whose side lengths are $c_1, c_2, \ldots, c_m$, where m is any integer with $m \geq 3$. Then we have

$$S(1,1,2,3,4,t,\ldots,t) = S(1,1,2,3,u) + S(u,4,t,\ldots,t)\,. \tag{16}$$

In this equation, we are considering a cyclic n-gon $B_1B_2\ldots B_n$ with $\overline{B_1B_2} = \overline{B_2B_3} = 1$, $\overline{B_3B_4} = 2$, $\overline{B_4B_5} = 3$, $\overline{B_5B_6} = 4$, $\overline{B_6B_1} = t$ if $n = 6$, or $\overline{B_6B_7} = t$, $\ldots$, $\overline{B_{n-1}B_n} = t$, $\overline{B_nB_1} = t$ if $n \geq 7$. (See Figure 2.) Thus in equation (16), the number of t's on each side is $n-5$. Also u denotes the diagonal length $u = \overline{B_1B_5}$, which is a function of t. It is geometrically clear that

$$\lim_{t\to+0} u = 4\,, \tag{17}$$

and that

$$\lim_{t\to+0} S(u,4,t,\ldots,t) = 0\,. \tag{18}$$

By Proposition 5 in Appendix A, $S(c_1, c_2, \ldots, c_m)$ is a continuous function of $(c_1, c_2, \ldots, c_m)$. Thus by (17), we have

$$\lim_{t\to+0} S(1,1,2,3,u) = S(1,1,2,3,4) = S_0\,. \tag{19}$$

Assumption $(\star)$ implies that

$$F(1,1,2,3,4,t,\ldots,t) = S(1,1,2,3,4,t,\ldots,t)\,.$$

Thus by (16), (18) and (19) we have

$$\lim_{t\to+0} F(1,1,2,3,4,t,\ldots,t) = S_0\,. \tag{20}$$

Proposition 2 is now proved. $\square$

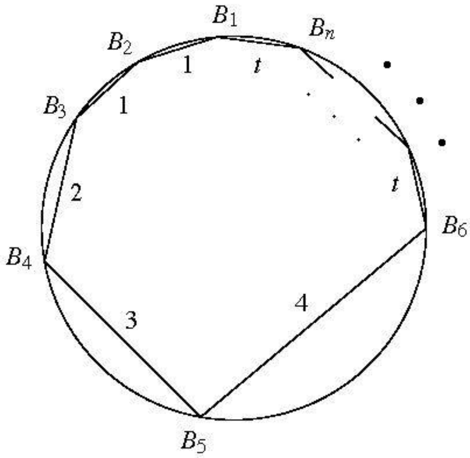

FIGURE 2
Cyclic n-gon $B_1B_2 \dots B_{n-1}B_n$

By Assumption ($\star$), the value $F(1,1,2,3,4,t,\dots,t)$ can be calculated by starting from rational numbers and the variable t, and applying the four arithmetic operations and taking k-th roots. In other words, $F(1,1,2,3,4,t,\dots,t)$ is an *admissible function* as defined in Appendix B. There we also define a *restricted admissible function* to be an admissible function which can be constructed from a finite number of polynomials in t with rational coefficients by using only *three* arithmetic operations of addition, subtraction, and multiplication (i.e. without using division), together with the operation of taking k-th roots.

For notational simplicity, let us denote $F(1,1,2,3,4,t,\dots,t)$ by $F(t)$. By Lemma 7 in Appendix B, an admissible function $F(t)$ can be expressed as a quotient of two restricted admissible functions:

$$F(t) = \frac{f(t)}{g(t)}, \tag{21}$$

where $f(t)$ and $g(t)$ are certain branches of restricted admissible functions which are not identically zero. Note that the domain of $F(t)$ contains a small interval $0 < t < \epsilon$. If ϵ is sufficiently small, this interval is contained in *unramified domains* (in the sense of Appendix B) of $f(t)$, $g(t)$ and $\sqrt[k]{t}$. We can choose a connected and simply connected open set D ($\subset \mathbf{C}$) which contains the interval $0 < t < \epsilon$ and serves as an unramified domain for all these functions simultaneously. We assume that on D a branch (denoted by $t^{\frac{1}{k}}$) of $\sqrt[k]{t}$ is selected so that $t^{\frac{1}{k}} > 0$ for $0 < t < \epsilon$. Then by Proposition 7 in Appendix B, the functions $f(t)$ and $g(t)$ have Puiseux expansions

(22) $$f(t) = c_0 + c_1 t^{\frac{1}{p}} + c_2 t^{\frac{2}{p}} + \cdots, \; 0 < t < \epsilon,$$

(23) $$g(t) = d_0 + d_1 t^{\frac{1}{q}} + d_2 t^{\frac{2}{q}} + \cdots, \; 0 < t < \epsilon,$$

where p and q are positive integers, and all the coefficients c_i, d_j belong to a radical extension of $\mathbf{Q}$.

Since $F(t)$ is the quotient of $f(t)$ and $g(t)$ (see (21)), and its limit when $t \to +0$ is a finite non-zero number S_0 (see (15)), we infer that the first non-zero terms of (22) and (23), say $c_i t^{\frac{i}{p}}$ and $d_j t^{\frac{j}{q}}$, have the same exponents:

$$\frac{i}{p} = \frac{j}{q}.$$

Then by cancelling $t^{\frac{i}{p}} = t^{\frac{j}{q}}$ from the numerator and the denominator, we have

$$F(t) = \frac{c_i + c_{i+1} t^{\frac{1}{p}} + c_{i+2} t^{\frac{2}{p}} + \cdots}{d_j + d_{j+1} t^{\frac{1}{q}} + d_{j+2} t^{\frac{2}{q}} + \cdots}, \quad 0 < t < \epsilon.$$

This implies that

(24) $$\lim_{t \to +0} F(t) = \frac{c_i}{d_j},$$

which belongs to a radical extension of $\mathbf{Q}$. Since by (15) this limit is equal to S_0, (24) contradicts the fact (proved in §2) that S_0 does not belong to any radical extension of $\mathbf{Q}$. This contradiction shows that Assumption ($\star$) is absurd. This proves Theorem 1 for $n \geq 6$. □

We would like to remark that Theorem 1 for $n = 5$ does not trivially imply Theorem 1 for $n \geq 6$. The following proposition seems to indicate the subtlety of the problem.

We have shown in §2 that for certain cyclic pentagons $ABCDE$ with $\overline{AB} = \overline{AE}$, there is no formula which gives the area in terms of the side lengths using only arithmetic operations and k-th roots. However, if $ABCDE$ is any cyclic pentagon with $\overline{AB} = \overline{AE}$, and if F is any point (other than A or E) on the arc AE of the circumscribed circle (as in Figure 3), then we can prove:

PROPOSITION 3. *There exists a formula which gives the area of the cyclic hexagon $ABCDEF$ (of Figure 3) in terms of its side lengths, using only arithmetic operations and square roots.*

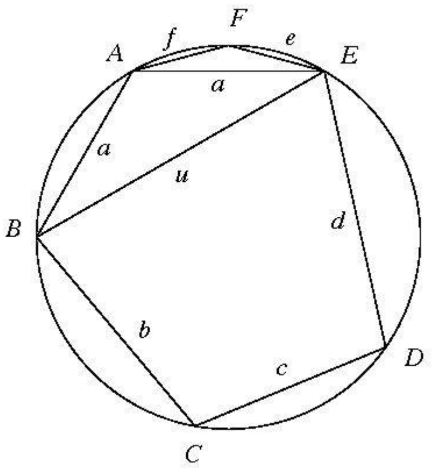

FIGURE 3
Cyclic pentagon $ABCDE$ and point F

Proof. Consider the cyclic quadrilateral $ABEF$ and its diagonal AE. Let u denote the length of the chord BE. By calculating $\overline{AE}^2$ as we did for x^2 in the proof of Lemma 2, we have

$$\overline{AE}^2 = \frac{(e^2+f^2)au+(a^2+u^2)ef}{au+ef}. \tag{25}$$

But $\overline{AE} = a$; after some simplifications we get

$$u = \frac{a(a^2-e^2-f^2)}{ef}. \tag{26}$$

Since the quadrilaterals $ABEF$ and $BCDE$ are cyclic, their areas can be calculated (by Brahmagupta's formula) from the side lengths a, u, e, f and b, c, d, u, respectively, using only arithmetic operations and square roots. This together with (26) completes the proof of Proposition 3. □

6. APPENDIX A

The purpose of this appendix is to prove two propositions on cyclic polygons, which are probably well-known, but are used in our arguments.

PROPOSITION 4. *Let n be an integer greater than 2. Let a_i, $i = 1, 2, \ldots, n$, be positive real numbers. The following three conditions are equivalent:*

(i) $2\max(a_1, a_2, \ldots, a_n) < \sum_{i=1}^{n} a_i$, *in other words,* $s - a_i > 0$ *for each* $i = 1, 2, \ldots, n$, *where* $s = (a_1 + a_2 + \ldots + a_n)/2$,

(ii) *there exists an* n*-gon whose side lengths are* $a_1, a_2, \ldots, a_n$,

(iii) *there exists a cyclic* n*-gon whose side lengths are* $a_1, a_2, \ldots, a_n$.

Proof. The implications (iii) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (i) are obvious. We will prove that (i) $\Rightarrow$ (iii).

Assume condition (i). We may assume that

$$a_n = \max(a_1, a_2, \ldots, a_n).$$

Then (i) is equivalent to

$$a_n < a_1 + a_2 + \ldots + a_{n-1}. \tag{27}$$

For $r > 0$, let $C(r)$ denote a circle of radius r. If A and B are two points on $C(r)$ and $a = \overline{AB}$, then the angle at the center of $C(r)$ subtended by the chord AB is

$$2\arcsin\left(\frac{a}{2r}\right), \tag{28}$$

where we choose the branch of arcsin so that

$$-\frac{\pi}{2} \leq \arcsin(x) \leq \frac{\pi}{2}, \quad \text{for} \quad -1 \leq x \leq 1.$$

To prove the implication (i) $\Rightarrow$ (iii), we consider three cases:

(A) $\sum_{i=1}^{n-1} \arcsin\left(\frac{a_i}{a_n}\right) > \frac{\pi}{2}$,

(B) $\sum_{i=1}^{n-1} \arcsin\left(\frac{a_i}{a_n}\right) = \frac{\pi}{2}$,

(C) $\sum_{i=1}^{n-1} \arcsin\left(\frac{a_i}{a_n}\right) < \frac{\pi}{2}$.

CASE (A). Note that if $C(r)$ circumscribes an n-gon whose side lengths are $a_1, a_2, \ldots, a_n$, then the diameter $2r$ must satisfy

$$2r \geq \max(a_1, a_2, \ldots, a_n) = a_n,$$

that is, $r \geq \frac{a_n}{2}$.

Consider the continuous function $f(r)$ defined by

$$f(r) = \sum_{i=1}^{n} \arcsin\left(\frac{a_i}{2r}\right), \quad r \geq \frac{a_n}{2}. \tag{29}$$

By assumption (A), we have

$$f(\frac{a_n}{2}) = \sum_{i=1}^{n-1} \arcsin\Big(\frac{a_i}{a_n}\Big) + \arcsin\Big(\frac{a_n}{a_n}\Big) > \frac{\pi}{2} + \frac{\pi}{2} = \pi\,.$$

By (29), we have

$$\lim_{r\to\infty} f(r) = 0\,.$$

Since

$$f'(r) = \sum_{i=1}^{n} \frac{-a_i}{r\sqrt{4r^2 - a_i^2}} < 0, \quad \text{for} \quad r > \frac{a_n}{2}\,, \tag{30}$$

the function $f(r)$ is monotone decreasing. Therefore, there exists a unique value r_0 $(> \frac{a_n}{2})$ such that $f(r_0) = \pi$, i.e.

$$\sum_{i=1}^{n} \arcsin\Big(\frac{a_i}{2r_0}\Big) = \pi\,. \tag{31}$$

Equation (31) means that the sum of the angles at the center of $C(r_0)$ subtended by the chords of lengths $a_1, a_2, \ldots, a_n$ is 2π. (See (28).) Thus there exists an n-gon with side lengths $a_1, a_2, \ldots, a_n$ inscribed in the circle $C(r_0)$. Case (A) is done.

CASE (B). Take n points $A_1, A_2, \ldots, A_n$, in this order, on the circle $C\big(\frac{a_n}{2}\big)$ of radius $\frac{a_n}{2}$ in such a way that $\overline{A_iA_{i+1}} = a_i$, for $i = 1, 2, \ldots, n-1$. Then by assumption (B), the sum of the central angles subtended by the chords $A_1A_2, A_2A_3, \ldots, A_{n-1}A_n$ is equal to π. Thus the chord A_1A_n is a diameter of $C\big(\frac{a_n}{2}\big)$, and its length is equal to a_n. This implies that the n-gon $A_1A_2\ldots A_n$ inscribed in $C\big(\frac{a_n}{2}\big)$ has the required side lengths $a_1, a_2, \ldots, a_n$. This concludes Case (B).

CASE (C). Take n points $A_1, A_2, \ldots, A_n$, in this order, on the circle $C(r)$ of radius r, where $r \geq \frac{a_n}{2}$. We take them so that $\overline{A_iA_{i+1}} = a_i$, for $i = 1, 2, \ldots, n-1$. The length of the chord A_1A_n depends on r, while the lengths of $A_1A_2, A_2A_3, \ldots, A_{n-1}A_n$ are fixed as above, independently of r. We denote the length of A_1A_n, as a continuous function of r, by $g(r)$. It is defined for $r \geq \frac{a_n}{2}$. Assumption (C) implies that if $r = \frac{a_n}{2}$ the sum of the angles at the center of $C\big(\frac{a_n}{2}\big)$, subtended by $A_1A_2, A_2A_3, \ldots, A_{n-1}A_n$, is less than π. Thus if $r = \frac{a_n}{2}$ the chord A_1A_n is shorter than the diameter of $C\big(\frac{a_n}{2}\big)$, that is,

$$g\Big(\frac{a_n}{2}\Big) < a_n\,. \tag{32}$$

As we show below, the function $g(r)$ is monotone increasing, and it is geometrically clear that

$$\lim_{r\to\infty} g(r) = \sum_{i=1}^{n-1} a_i . \tag{33}$$

Recall that by (27),

$$a_n < \sum_{i=1}^{n-1} a_i . \tag{34}$$

Then by (32), (33), (34), we infer that there exists a unique value r_0 such that $r_0 > \frac{a_n}{2}$ and $g(r_0) = a_n$; in other words, we have

$$\overline{A_1A_n} = a_n ,$$

on the circle $C(r_0)$. This implies that the n-gon $A_1A_2\ldots A_n$ inscribed in the circle $C(r_0)$ has the required side lengths $a_1, a_2, \ldots, a_n$. This concludes Case (C) except for the proof that $g(r)$ is monotone increasing.

We now prove this fact. Let O denote the center of $C(r)$. By assumption (C), we have

$$\angle A_1OA_n = 2\sum_{i=1}^{n-1} \arcsin\left(\frac{a_i}{2r}\right) < \pi, \quad \text{for} \quad r \geq \frac{a_n}{2} , \tag{35}$$

and the function $g(r)$ is written explicitly as

$$g(r) = 2r\sin\left(\frac{\angle A_1OA_n}{2}\right) = 2r\sin\left(\sum_{i=1}^{n-1} \arcsin\left(\frac{a_i}{2r}\right)\right) . \tag{36}$$

For simplicity, we set

$$\theta_i = \arcsin\left(\frac{a_i}{2r}\right) .$$

Then we have

$$g'(r) = 2\sin\left(\sum_{i=1}^{n-1}\theta_i\right) + 2r\cos\left(\sum_{i=1}^{n-1}\theta_i\right)\left(\sum_{i=1}^{n-1}\frac{-a_i}{r\sqrt{4r^2-a_i^2}}\right) .$$

As is clear from Figure 4, we have

$$\frac{a_i}{\sqrt{4r^2-a_i^2}} = \tan\theta_i . \tag{37}$$

Substituting (37), we have

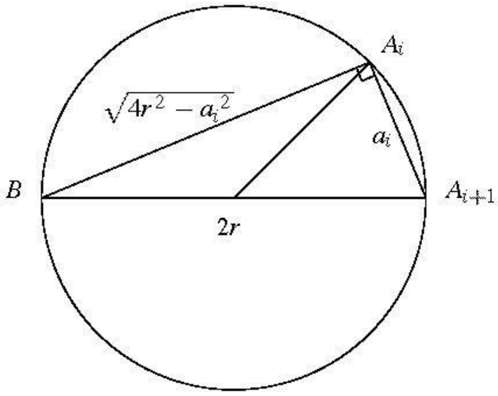

FIGURE 4
$\theta_i = \angle A_iBA_{i+1} = \arcsin\left(\frac{a_i}{2r}\right)$, and $\overline{A_iB} = \sqrt{4r^2 - a_i^2}$

$$
\begin{aligned}
(38) \qquad g'(r) &= 2\sin\Big(\sum_{i=1}^{n-1}\theta_i\Big) - 2\cos\Big(\sum_{i=1}^{n-1}\theta_i\Big)\Big(\sum_{i=1}^{n-1}\tan\theta_i\Big) \\
&> 2\sin\Big(\sum_{i=1}^{n-1}\theta_i\Big) - 2\cos\Big(\sum_{i=1}^{n-1}\theta_i\Big)\tan\Big(\sum_{i=1}^{n-1}\theta_i\Big) = 0\,.
\end{aligned}
$$

Note that we used the fact that $0 < \theta_i < \sum_{i=1}^{n-1}\theta_i < \frac{\pi}{2}$ in the above computation. See (35).

Thus we have proved that $g'(r) > 0$ for $r \geq \frac{a_n}{2}$, i.e that $g(r)$ is monotone increasing, as asserted. This completes the proof of Proposition 4. □

Let D_n be the open set in n-dimensional space $\mathbf{R}^n$ defined as follows:

$$
D_n = \Big\{(a_1, a_2, \ldots, a_n) \mid a_1 > 0, \ldots, a_n > 0,\ 2\max(a_1, a_2, \ldots, a_n) < \sum_{i=1}^{n} a_i\Big\}.
$$

By Proposition 4, for each $(a_1, a_2, \ldots, a_n) \in D_n$ there exists a cyclic n-gon whose side lengths are $a_1, a_2, \ldots, a_n$. Let $S(a_1, a_2, \ldots, a_n)$ denote the area of such a cyclic n-gon.

PROPOSITION 5. *$S(a_1, a_2, \ldots, a_n)$ is a continuous function on D_n.*

Though this proposition seems intuitively clear, we will give a proof for completeness. Before proving Proposition 5, we will prove a closely related lemma.

Let r denote the radius of the circumscribed circle of a cyclic n-gon with side lengths $a_1, a_2, \ldots, a_n$.

LEMMA 6. *r is a continuous function on D_n.*

Proof. We divide D_n into $n+1$ subsets $\mathcal{A}, \mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_n$ defined as follows:

$$\mathcal{A} = \left\{(a_1, a_2, \ldots, a_n) \,\Big|\, \sum_{i=1}^{n} \arcsin\Big(\frac{a_i}{M}\Big) \geq \pi\right\}, \text{ where } M = \max(a_1, a_2, \ldots, a_n),$$

$$\mathcal{C}_j = \left\{(a_1, a_2, \ldots, a_n) \,\Big|\, a_j = \max(a_1, a_2, \ldots, a_n) \text{ and } \sum_{i\,(i\neq j)} \arcsin\Big(\frac{a_i}{a_j}\Big) \leq \frac{\pi}{2}\right\}.$$

Note that

$$D_n = \mathcal{A} \cup \mathcal{C}_1 \cup \mathcal{C}_2 \cup \ldots \cup \mathcal{C}_n .$$

From the arguments of Cases (B) and (C) in the proof of Proposition 4, it is clear that if $(a_1, a_2, \ldots, a_n) \in \mathcal{C}_j$, then

$$a_j > a_k, \quad \text{for} \quad \forall k \in \{1, 2, \ldots, n\} \setminus \{j\}.$$

Thus if $j \neq k$, then

$$\mathcal{C}_j \cap \mathcal{C}_k = \varnothing .$$

Also note that

$$\mathcal{A} \cap \mathcal{C}_j = \left\{(a_1, a_2, \ldots, a_n) \mid \sum_{i\,(i\neq j)} \arcsin\Big(\frac{a_i}{a_j}\Big) = \frac{\pi}{2}\right\},$$

because if $M = a_j$, then $\arcsin\big(\frac{a_j}{M}\big) = \arcsin(1) = \frac{\pi}{2}$.

Suppose that

$$(a_1, a_2, \ldots, a_n) \in \operatorname{int}(\mathcal{A}) = \mathcal{A} \setminus \Big(\bigcup_j \mathcal{A} \cap \mathcal{C}_j\Big).$$

Then from the argument of Case (A) in the proof of Proposition 4, r is uniquely determined by the condition $f(r) = \pi$, where $f(r)$ is the function defined by (29). Differentiating $f(r)$, we have $f'(r) < 0$ (see (30)).

Thus by the implicit function theorem, the value of r satisfying $f(r) = \pi$ depends smoothly on $(a_1, a_2, \ldots, a_n)$. We denote this function by

$$r = \varphi_{\mathcal{A}}(a_1, a_2, \ldots, a_n), \quad (a_1, a_2, \ldots, a_n) \in \operatorname{int}(\mathcal{A}).$$

If a point $(a_1, a_2, \ldots, a_n) \in \operatorname{int}(\mathcal{A})$ approaches the boundary $\mathcal{A} \cap \mathcal{C}_j$, that is, if $a_j = \max(a_1, a_2, \ldots, a_n)$, and

$$\sum_{i\,(i\neq j)} \arcsin\left(\frac{a_i}{a_j}\right) \to \frac{\pi}{2} + 0,$$

then from Case (A) in the proof of Proposition 4, we have

$$\varphi_{\mathcal{A}}(a_1, a_2, \ldots, a_n) \to \frac{a_j}{2}.$$

On the other hand, from Case (B) in the proof of Proposition 4, it is clear that the radius of the circumscribed circle of a polygon corresponding to a point $(a_1, a_2, \ldots, a_n) \in \mathcal{A} \cap \mathcal{C}_j$ is equal to $\frac{a_j}{2}$. Therefore, the smooth function $\varphi_{\mathcal{A}}$ on $\mathrm{int}(\mathcal{A})$ is continuously extended to $\mathcal{A}$ by defining

$$\varphi_{\mathcal{A}}(a_1, a_2, \ldots, a_n) = \frac{a_j}{2}, \quad (a_1, a_2, \ldots, a_n) \in \mathcal{A} \cap \mathcal{C}_j. \tag{39}$$

Next suppose that

$$(a_1, a_2, \ldots, a_n) \in \mathrm{int}(\mathcal{C}_j) = \mathcal{C}_j \setminus (\mathcal{A} \cap \mathcal{C}_j).$$

Then $a_j = \max(a_1, a_2, \ldots, a_n)$, and the radius r of the circumscribed circle is uniquely determined by the condition $g(r) = a_j$, where $g(r)$ is a function explicitly given by

$$g(r) = 2r \sin\left(\sum_{i\,(i\neq j)} \arcsin\left(\frac{a_i}{2r}\right)\right).$$

See equation (36) in Case (C) of the proof of Proposition 4, where it was assumed that $a_n = \max(a_1, a_2, \ldots, a_n)$. Since $g'(r) > 0$ by (38), the implicit function theorem tells us that the radius r is a smooth function of $(a_1, a_2, \ldots, a_n) \in \mathrm{int}(\mathcal{C}_j)$. Let us denote this function by

$$r = \varphi_j(a_1, a_2, \ldots, a_n), \quad (a_1, a_2, \ldots, a_n) \in \mathrm{int}(\mathcal{C}_j) \ (= \mathcal{C}_j \setminus \mathcal{A} \cap \mathcal{C}_j).$$

If a point $(a_1, a_2, \ldots, a_n) \in \mathrm{int}(\mathcal{C}_j)$ approaches the boundary $\mathcal{A} \cap \mathcal{C}_j$, that is, if

$$\sum_{i\,(i\neq j)} \arcsin\left(\frac{a_i}{a_j}\right) \to \frac{\pi}{2} - 0,$$

then from Case (C) of the proof of Proposition 4, we have

$$\varphi_j(a_1, a_2, \ldots, a_n) \to \frac{a_j}{2}.$$

Thus as in the case of $\varphi_{\mathcal{A}}$, the smooth function φ_j on $\mathrm{int}(\mathcal{C}_j)$ is continuously extended to $\mathcal{C}_j$ by defining

$$\varphi_j(a_1, a_2, \ldots, a_n) = \frac{a_j}{2}, \quad (a_1, a_2, \ldots, a_n) \in \mathcal{A} \cap \mathcal{C}_j. \tag{40}$$

By (39) and (40), we have for $j = 1, 2, \ldots, n$

$$\varphi_{\mathcal{A}}(a_1, a_2, \ldots, a_n) = \varphi_j(a_1, a_2, \ldots, a_n), \qquad \forall (a_1, a_2, \ldots, a_n) \in \mathcal{A} \cap \mathcal{C}_j.$$

Therefore, by gluing togther $\varphi_{\mathcal{A}}$, and φ_j, $j = 1, 2, \ldots, n$, we obtain a continuous function $r = \varphi(a_1, a_2, \ldots, a_n)$ on D_n. This proves Lemma 6. $\square$

Once Lemma 6 is proved, Proposition 5 is easy to prove.

Proof of Proposition 5. The area $S(a_1, a_2, \ldots, a_n)$ is calculated as follows:

$$S(a_1, a_2, \ldots, a_n) = \begin{cases} \sum_{i=1}^{n} \frac{a_i}{2}\sqrt{r^2 - \frac{a_i^2}{4}} & \text{on } \mathcal{A}, \\ \sum_{i\,(i \neq j)} \frac{a_i}{2}\sqrt{r^2 - \frac{a_i^2}{4}} - \frac{a_j}{2}\sqrt{r^2 - \frac{a_j^2}{4}} & \text{on } \mathcal{C}_j. \end{cases}$$

These two expressions coincide on the boundary $\mathcal{A} \cap \mathcal{C}_j$, because we have $r = \frac{a_j}{2}$ there. Since r depends on $(a_1, a_2, \ldots, a_n)$ continuously, $S(a_1, a_2, \ldots, a_n)$ also depends continuously on $(a_1, a_2, \ldots, a_n)$. This completes the proof of Proposition 5. □

7. APPENDIX B

The purpose of this appendix is to discuss "Puiseux expansions" of *complex valued* algebraic functions of one *complex* variable, used in the proof of Theorem 1. For an explanation of Puiseux expansions, see [8].

We will denote by $\mathbf{Q}[t]$ the polynomial ring of a variable t with rational coefficients, and by $\mathbf{Q}(t)$ the quotient field of $\mathbf{Q}[t]$. In other words, $\mathbf{Q}(t)$ is the field of rational functions of a variable t with rational coefficients.

In this appendix, our discussion will be confined to rather special types of algebraic functions.

DEFINITION. An algebraic function $F(t)$ is said to be an *admissible function* if it belongs to a radical extension of the field $\mathbf{Q}(t)$.

This means that a function $F(t)$ is admissible if and only if it is constructed from a finite number of polynomial functions ($\in \mathbf{Q}[t]$) by using the four arithmetic operations, together with the operation of taking k-th roots.

Note that when taking a k-th root of a function $f(t)$,

$$\sqrt[k]{f(t)}\,, \tag{41}$$

we meet the ambiguity that the value is only determined up to multiplication by k-th roots of unity. In other words, the expression (41) may be any one of the following k functions (*branches*)

$$\sqrt[k]{f(t)},\ \zeta\sqrt[k]{f(t)}, \ldots, \zeta^{k-1}\sqrt[k]{f(t)}\,, \tag{42}$$

where ζ is a primitive k-th root of unity. In some special cases, we can remove this ambiguity. For example, take a connected and simply connected region D in the complex number plane $\mathbf{C}$, so that D does not contain any zeros of $f(t)$ nor of $1/f(t)$, and restrict the variable t within D, then we can remove the ambiguity of (41) in the sense that we can choose as we like one of the branches from (42) over the domain D without any ambiguity.

We will later show how to take a useful domain D in our application. However, before that, we will consider an admissible function to be a multi-valued function.

DEFINITION. An admissible function $F(t)$ is said to be of *restricted type* or briefly a *restricted* admissible function, if we can construct it from a finite number of polynomials ($\in \mathbf{Q}[t]$) by using only the *three* arithmetic operations of addition, subtraction, and multiplication (i.e. without using division), together with the operation of taking k-th roots.

For example, a polynomial function ($\in \mathbf{Q}[t]$) is a restricted admissible function.

It is easy to see that the next lemma holds.

LEMMA 7. *Every admissible function can be expressed as a quotient of two restricted admissible functions.*

A polynomial in an indeterminate X is said to be *monic*, if the coefficient of the leading term X^m is 1.

LEMMA 8. *A restricted admissible function $F(t)$ which is not identically zero satisfies a monic polynomial equation whose coefficients belong to $\mathbf{Q}[t]$. More precisely, given a non-zero restricted admissible function $F(t)$, there exists a monic polynomial equation*

$$X^m + f_1 X^{m-1} + \cdots + f_{m-1} X + f_m = 0 \tag{43}$$

with $f_i \in \mathbf{Q}[t]$, $i = 1, 2, \ldots, m$, such that $X = F$ is one of its solutions, that is,

$$F^m + f_1 F^{m-1} + \cdots + f_{m-1} F + f_m = 0 \tag{44}$$

holds identically as a function of t.

This lemma can be proved by arguments similar to those in Chapter I, §2 of [3].

For a given $F(t)$, choosing a polynomial equation (43) with the lowest degree m, we may assume that f_m is not a zero polynomial. This is because if $f_m = 0$, then $F(t)$ would satisfy a polynomial equation of lower degree

$$F^{m-1} + f_1 F^{m-2} + \cdots + f_{m-1} = 0\,.$$

The following proposition is in fact a corollary of Lemma 8.

PROPOSITION 6. *A restricted admissible function $F(t)$ which is not identically zero has a finite number of zeros.*

Proof. Suppose that $F(t)$ satisfies equation (43), i.e. that equation (44) holds identically as a function of t. Suppose that $F(t_0) = 0$ for some $t_0 \in \mathbf{C}$. Then from (44), we have

$$f_m(t_0) = 0\,.$$

Thus the zero set of F is a subset of the zero set of f_m. Since a polynomial f_m has a finite number of zeros, this proves Proposition 6. $\square$

Let $F(t)$ be a restricted admissible function which is not identically zero. We define an *inductive sequence for constructing* $F(t)$ to be a sequence consisting of a finite number of non-zero restricted admissible functions

$$\mathcal{I}(F(t)) = \{F_1, F_2, \ldots, F_N\} \tag{45}$$

which satisfies the following conditions (a) and (b):

(a) F_1 is a polynomial in t with rational coefficients, and $F_N = F(t)$, the given restricted admissible function,

(b) each $F_h (h = 2, \ldots, N)$ is a polynomial in t with rational coefficients, or $F_h = F_i \pm F_j$, $F_h = F_i F_j$, or $F_h = \sqrt[k]{F_i}$, where F_i and F_j are functions in the sequence $\mathcal{I}(F(t))$ which appear before F_h. Furthermore, for each such h, the indices i and j are explicitly specified.

Suppose we are given a non-zero restricted admissible function $F(t)$. Then fixing a certain inductive sequence $\mathcal{I}(F(t))$ for constructing it, we define the *set of ramification points* of $F(t)$, denoted by $Ram(F)$ $(\subset \mathbf{C})$, inductively as follows:

(i) If $F_h (\in \mathcal{I}(F(t)))$ is a polynomial in t with rational coefficients, we set

$$Ram(F_h) = \varnothing\,,$$

(ii) if $F_h = F_i \pm F_j$ or $F_h = F_i F_j$, where F_i and F_j are specified non-zero restricted admissible functions in the sequence $\mathcal{I}(F(t))$ appearing before F_h, then we set

$$Ram(F_h) = Ram(F_i) \cup Ram(F_j)\,,$$

(iii) if $F_h = \sqrt[k]{F_i}$ with a specified restricted admissible function F_i which appears before F_h in the sequence $\mathcal{I}(F(t))$, and $k > 1$, then we set

$$Ram(F_h) = Ram(F_i) \cup Zero(F_i)\,.$$

where $Zero(F_i)$ is the zero set of F_i.

REMARK. We adopt the convention that if in the inductive sequence $\mathcal{I}(F(t))$ a function F_h is a polynomial in t with rational coefficients, and at the same time, the construction of F_h is explicitly specified as $F_h = F_i \pm F_j$, $F_h = F_iF_j$ or $F_h = \sqrt[k]{F_i}$, then to define $Ram(F_h)$ we apply rule (ii) or (iii) rather than (i).

Although the notation is somewhat imprecise, the set $Ram(F(t))$ depends not only on $F(t)$ but also on $\mathcal{I}(F(t))$. When we speak of the set of ramification points of $F(t)$, we always assume tacitly that a certain inductive sequence (45) for constructing $F(t)$ has been chosen and fixed. By the definition of a restricted admissible function and Proposition 6, $Ram(F)$ is a finite set of points ($\subset \mathbf{C}$).

DEFINITION. Let $F(t)$ be a restricted admissible function which is not identically zero. An open set D ($\subset \mathbf{C}$) is said to be an *unramified domain* for $F(t)$, if D is connected and simply connected, and satisfies $D \cap Ram(F) = \varnothing$.

If D is an unramified domain for a restricted admissible function $F(t)$, then $F(t)$ restricted to D is a disjoint union of a finite number of branches, each of which is a univalent function over D.

For example, if D is a connected and simply connected open set which does not contain 0, then D is an unramified domain for $\sqrt[k]{t}$, for any $k \geq 1$. Moreover, if D contains an open interval $(0, \epsilon)$ ($\subset \mathbf{R}$) with a small $\epsilon > 0$, then we can uniquely select a branch of the function $\sqrt[k]{t}$ over D such that

$$\sqrt[k]{t} > 0\,, \quad \text{for each } t \in (0, \epsilon)\,. \tag{46}$$

We will denote this branch by $t^{\frac{1}{k}}$.

In the following proposition, D_ϵ denotes the connected component of $\{t \in \mathbf{C} \mid |t| < \epsilon\} \cap D$ which contains $(0, \epsilon)$.

PROPOSITION 7. *Let $F(t)$ be a restricted admissible function which is not identically zero. Let D be an unramified domain for $F(t)$. Suppose that D does not contain 0, but contains an open interval $(0,\epsilon)$ with a sufficiently small $\epsilon > 0$. Then for each branch of $F(t)$ over D, there exists an integer $p > 0$ such that the branch can be expanded as follows:*

$$F(t) = c_0 + c_1 t^{\frac{1}{p}} + c_2 t^{\frac{2}{p}} + \cdots, \qquad \text{for } t \in D_\epsilon. \tag{47}$$

Furthermore, for a fixed $F(t)$, all the coefficients c_i belong to a radical extension of $\mathbf{Q}$.

The expansion (47) is called the *Puiseux expansion* of $F(t)$.

Proof. Let $\mathcal{I}(F(t))$ be the inductive sequence for constructing $F(t)$ which is tacitly assumed. We will prove Proposition 7 by induction based on $\mathcal{I}(F(t))$, starting from a polynomial $\in \mathbf{Q}[t]$. Note that by the definition of an unramified domain for a restricted admissible function, the unramified domain D for $F(t)$ also serves as an unramified domain for all the functions which appear in the inductive sequence $\mathcal{I}(F(t))$.

A polynomial $f(t) \in \mathbf{Q}[t]$ has a natural Puiseux expansion:

$$f(t) = a_0 + a_1 t + \cdots + a_m t^m,$$

in which all the coefficients $a_0, a_1, \ldots, a_m$ belong to $\mathbf{Q}$.

Suppose that branches of two restricted admissible functions $f(t)$, $g(t)$ have Puiseux expansions:

$$f(t) = a_0 + a_1 t^{\frac{1}{p}} + a_2 t^{\frac{2}{p}} + \cdots, \tag{48}$$

$$g(t) = b_0 + b_1 t^{\frac{1}{q}} + b_2 t^{\frac{2}{q}} + \cdots, \tag{49}$$

in which $a_0, a_1, a_2, \ldots$ belong to a radical extension K_1 of $\mathbf{Q}$, and $b_0, b_1, b_2, \ldots$ belong to another radical extension K_2 of $\mathbf{Q}$. If $f(t) \neq -g(t)$, then the sum $f(t) + g(t)$ is not identically zero, and has a Puiseux expansion

$$f(t) + g(t) = c_0 + c_1 t^{\frac{1}{r}} + c_2 t^{\frac{2}{r}} + \cdots,$$

where $r = \text{l.c.m.}(p, q)$, and $c_i = 0, a_j, b_j$, or $a_j + b_k$ as the case may be. Thus the coefficients $c_0, c_1, c_2, \ldots$ belong to a radical extension K_3 of $\mathbf{Q}$ generated by K_1, K_2. The argument for the difference $f(t) - g(t)$ is the same.

The product of $f(t)g(t)$ has a Puiseux expansion

$$f(t)g(t) = c_0 + c_1 t^{\frac{1}{r}} + c_2 t^{\frac{2}{r}} + \cdots,$$

where $r = pq$, and

$$c_i = \sum a_j b_k ,$$

with the indices j, k running over all pairs (j, k) that satisfy $\frac{j}{p} + \frac{k}{q} = \frac{i}{r}$. (If for some i no such pair exists, then $c_i = 0$.) Obviously, the coefficients $c_0, c_1, c_2, \ldots$ belong to a radical extension K_3 of $\mathbf{Q}$ generated by K_1, K_2.

Finally, let us consider a branch of k-th roots of $f(t)$. We assume that $f(t)$ has Puiseux expansion (48) whose coefficients $a_0, a_1, a_2, \ldots$ belong to a radical extension K_1 of $\mathbf{Q}$. Let n be the smallest index such that $a_n \neq 0$. Then we have

$$\begin{aligned} \sqrt[k]{f(t)} &= \sqrt[k]{a_n t^{\frac{n}{p}} + a_{n+1} t^{\frac{n+1}{p}} + \cdots} \\ &= \sqrt[k]{a_n}\, t^{\frac{n}{pk}} \sqrt[k]{1 + \frac{a_{n+1}}{a_n} t^{\frac{1}{p}} + \frac{a_{n+2}}{a_n} t^{\frac{2}{p}} + \cdots} . \end{aligned} \tag{50}$$

Note that the value of $\sqrt[k]{a_n}$ is determined without ambiguity involving k-th roots of unity by the choice of the branch of $\sqrt[k]{f(t)}$ over D_ϵ, and $\sqrt[k]{a_n}$ belongs to a radical extension K_1' of K_1. Here K_1' is the radical extension of $\mathbf{Q}$ which is generated by K_1 and $\sqrt[k]{a_n}$.

Recall the binomial expansion:

$$\sqrt[k]{1+z} = \sum_{i=0}^{\infty} \binom{\frac{1}{k}}{i} z^i , \tag{51}$$

where

$$\binom{\frac{1}{k}}{i} = \begin{cases} \frac{1}{i!}\frac{1}{k}(\frac{1}{k}-1)\cdots(\frac{1}{k}-i+1) & i \geq 1, \\ 1 & i = 0 . \end{cases} \tag{52}$$

In particular, the binomial coefficients (52) belong to $\mathbf{Q}$.

The series (51) converges for $|z| < 1$. Thus if ϵ is sufficiently small, we have for $0 < t < \epsilon$:

$$\sqrt[k]{1 + \frac{a_{n+1}}{a_n} t^{\frac{1}{p}} + \frac{a_{n+2}}{a_n} t^{\frac{2}{p}} + \cdots} = \sum_{i=0}^{\infty} \binom{\frac{1}{k}}{i} \left(\frac{a_{n+1}}{a_n} t^{\frac{1}{p}} + \frac{a_{n+2}}{a_n} t^{\frac{2}{p}} + \cdots \right)^i . \tag{53}$$

Equation (53) shows that all the coefficients of the Puiseux expansion of

$$\sqrt[k]{1 + \frac{a_{n+1}}{a_n} t^{\frac{1}{p}} + \frac{a_{n+2}}{a_n} t^{\frac{2}{p}} + \cdots}$$

belong to K_1. Thus, by (50), $\sqrt[k]{f(t)}$ has a Puiseux expansion whose coefficients belong to a radical extension K_1' of $\mathbf{Q}$.

Therefore, Proposition 7 is proved by induction. □

REFERENCES

[1] BLASCHKE, W. *Kreis und Kugel.* Walter de Gruyter, Berlin, 1956. Reprint: Chelsea Publishing Company, New York, 1949.

[2] BOYER, C. B. *A History of Mathematics.* 2nd ed. (revised by U. C. Merzbach). John Wiley & Sons, Inc., 1991.

[3] LANG, S. *Algebraic Number Theory.* Graduate Texts in Math., Springer-Verlag, 1986.

[4] POSTNIKOV, M. M. *Foundations of Galois theory.* Translated by A. Swinfen, translation ed. P. J. Hilton. Pergamon Press, 1962.

[5] SWALLOW, J. *Exploratory Galois Theory.* Cambridge Univ. Press, 2004.

[6] VARFOLOMEEV, V. V. Inscribed polygons and Heron polynomials. *Sb. Mat. 194* (2003), 311–331.

[7] —— Galois groups of the Heron-Sabitov polynomials for pentagons inscribed in a circle. *Sb. Mat. 195* (2004), 149–162.

[8] WALL, C. T. C. *Singular Points of Plane Curves.* London Math. Soc. Student Texts *63*. Cambridge Univ. Press, 2004.

(Reçu le 10 janvier 2006; version révisée reçue le 10 mars 2007)

Yukio Matsumoto

Department of Mathematics
Faculty of Science
Gakushuin University
1-5-1 Mejiro, Toshima-ku
Tokyo 171-8588
Japan
e-mail: yukiomat@math.gakushuin.ac.jp

Yoshikazu Matsutani

3-21-1 Minamimachi
Kokubunji
Tokyo 185-0021
Japan
e-mail: ktbr-amrc@taupe.plala.or.jp

Tsuyoshi Sakai

Department of Mathematics
College of Humanities and Sciences
Nihon University, Setagaya-ku
Tokyo 156-0045
Japan

Masami Oda

Tsuda College, Kodaira
Tokyo 187-8577
Japan
e-mail: oda@tsuda.ac.jp

Tsukasa Shibuya

2-19-22-301 Nishiwaseda
Shinjuku-ku
Tokyo 169-0051
Japan