Constructible Numbers

Tyler Dunaisky, Adam Cohen, Blaze Okonogi-Neth

1 Introduction

Few things are more interesting than longstanding unsolved problems. And, when a mathematician solves one, the techniques used are worth their own mathematical merit. There are a few examples of such classical problems from the Greeks, all of which happen to involve one central concept: the usage of a straight-edge and compass. These problems go in the following way: with just a straight-edge and compass, can one construct

1. A square with area equal to that of a circle with unit radius?
2. An angle with measure one-third that of a given angle?
3. A cube with volume twice the volume of the unit cube?

Many of these related problems were not solved until the 19th century, where developments in field theory allowed for straightforward proofs of impossibility of such constructions due to the incredible fact that so-called "constructible numbers" form a subfield of $\mathbb{C}$! This fact can be leveraged to apply the full brunt of Galois theory to these problems. This brings us to our definitions. We define the **Constructible numbers** $\mathscr{C}$ as a subset of $\mathbb{C}$ containing 0 and 1 that is closed in the following way: we may formally construct geometric objects according to the following two axioms, and obtain new points from them according to another three axioms. The set of constructible numbers is then the set of points obtained in such a way. The axioms go as follows:

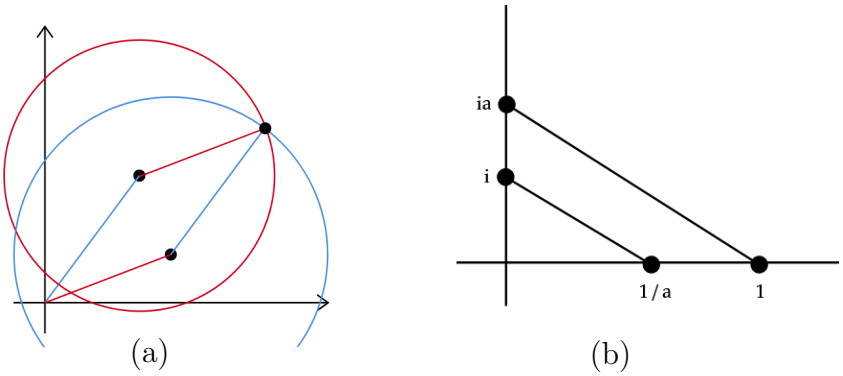
Definition. *Given two points $x, y \in \mathscr{C}$,*

- *SE 1: We may construct the infinite line that connects x and y.*
- *SE 2: We may construct the circle centered at x with radius determined by y.*

We then can further obtain new points in $\mathscr{C}$ from the following three axioms:

Definition.

- *If $x \in \mathbb{C}$ is at the intersection of two lines constructed from SE 1, then $x \in \mathscr{C}$.*
- *If $x \in \mathbb{C}$ is at the intersection of two circle constructed from SE 2, then $x \in \mathscr{C}$.*
- *If $x \in \mathbb{C}$ is at the intersection of a circle constructed from SE 2 and a line constructed from SE 1, then $x \in \mathscr{C}$.*



(a) (b)

Figure 1: (a) Constructing $\alpha + \beta$, (b) Constructing 1/a

From these definitions, it is immediately clear that we have every integer: construct the line between 0 and 1, and then construct a circle of radius 1 starting from either 0 or 1 repeatedly. Every integer can be realized as the intersection of a circle and this line.

From two applications of SE 2 centered at -1 and 1 with radius 2, we can then construct the perpendicular bisector, which is precisely the imaginary axis. From this we obtain i and $-i$, and thus the pure imaginary integers.

Theorem 1.1. *If $\alpha = a+ib$ for $a, b \in \mathbb{R}$, then $\alpha \in \mathscr{C}$ if and only if $a \in \mathscr{C}$ and $b \in \mathscr{C}$.*

Proof. Begin by noticing that a real number $b \in \mathbb{R} \cap \mathscr{C}$ if and only if $ib \in \mathscr{C}$ and $x \in \mathbb{R}$. Since a line on the y-axis may be constructed by dropping a perpendicular bisector to $[-1, 1]$, if $b \in \mathbb{R} \cap \mathscr{C}$, then the circle with center 0 and radius b intersects the imaginary axis at ib. Conversely, if ib is pure-imaginary and constructible, then, since a line along x-axis is constructible, the circle from 0 with radius determined by ib intersects this line at b, and so $b \in \mathbb{R} \cap \mathscr{C}$.

Let $\alpha = a+ib$. Assume that $a, b \in \mathscr{C} \cap \mathbb{R}$. Then $ib \in \mathscr{C}$, and so $a+ib \in \mathscr{C}$. Conversely, we may drop altitudes from α to the x-axis and y-axis respectively, and the points of intersection are a and ib respectively. Hence a and b are real and constructible. □

This theorem is the first step to realizing the constructible numbers. We will use it to prove the following fundamental result:

Theorem 1.2. *The set $\mathscr{C}$ of constructible numbers is a subfield of $\mathbb{C}$.*

Proof. We begin by verifying that $\mathscr{C}$ is closed under addition. Let α, β be two constructible numbers. Then one intersection of the circle with center α and radius β with the circle with center β and radius α is precisely $\alpha + \beta$.

We will now verify that if $a, b \in \mathbb{R} \cap \mathscr{C}$, then $1/a, ab \in \mathbb{R} \cap \mathscr{C}$. First, construct a line between a and i. Then, construct a parallel line from ib (which is constructible for reasons discussed above), and the point of intersection between this line and the real axis is ab. Similarly, drawing a line from ia to 1 and constructing a parallel through i intersects the real axis at $1/a$. So $ab, 1/a \in \mathbb{R} \cap \mathscr{C}$.

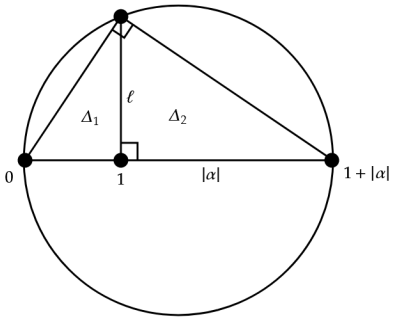


Figure 2: Constructing $\sqrt{|\alpha|}$

Finally, let $\alpha = a + ib \in \mathscr{C}$ and $\beta = c + id \in \mathscr{C}$. Then

$$\alpha\beta = (a + ib)(c + id) = (ac - bd) + i(ad + bc),$$

$$\frac{1}{\alpha} = \frac{\overline{\alpha}}{|\alpha|^2} = \frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2}.$$

By arguments above, $a, b, c, d \in \mathbb{R} \cap \mathscr{C}$. It follows that the real and imaginary parts of both $\alpha\beta$ and $1/\alpha$ are constructible, and so $\alpha\beta, 1/\alpha \in \mathscr{C}$. Hence $\mathscr{C}$ is a subfield of $\mathbb{C}$. □

From this theorem it is now clear that $\mathbb{C}/\mathscr{C}/\mathbb{Q}$. We now prove part of the characterizing property of the constructible numbers.

Theorem 1.3. *$\alpha \in \mathscr{C}$ implies $\sqrt{\alpha} \in \mathscr{C}$.*

Proof. To see that $\mathscr{C}$ is closed under square roots, we show that for $\alpha \in \mathscr{C}$, we also have $|\alpha|^{\frac{1}{2}} e^{\frac{i\theta}{2}}$, where θ is the principal argument of α. Then, the other square root is simply a reflection of the square root we construct through the origin, which is a simple task. So, from the comments above, it suffices to show that $\sqrt{|\alpha|}$ is a constructible real number and $e^{i\theta/2}$ is constructible.

Bisecting a given angle can be done using simple high school geometry, so $e^{i\theta/2} \in \mathscr{C}$. Now, $|\alpha|$ is constructible if $\alpha \in \mathbb{C}$, so we may construct $1 + |\alpha|$ and the circle at $(1 + |\alpha|)/2$ with radius determined by 0 using the field properties of $\mathscr{C}$. This looks something like the above drawing after dropping an altitude at 1. Then Δ_1 is similar to Δ_2, and so $1/\ell = \ell/|\alpha|$, so $\ell^2 = |\alpha|$. Thus $\ell = \sqrt{|\alpha|}$, and constructing a circle from 1 of radius ℓ gives us an intersection with the real axis at $1 + \sqrt{|\alpha|}$. Thus $\sqrt{|\alpha|} \in \mathscr{C}$, and consequently $\sqrt{\alpha} \in \mathscr{C}$. □

2 Structure of $\mathscr{C}$

The following theorem provides a useful connection between the geometry of constructible numbers and the theory of field extensions.

Theorem 2.1. *A complex number α is constructible if and only if there are extensions*

$$F_n/F_{n-1}/\cdots/F_1/F_0 = \mathbb{Q},$$

where the degree of each extension is 2 and $\alpha \in F_n$.

Proof. First, assume we have such a tower of extensions. Note that since $\alpha \in F_n$, it is sufficient to show $F_n \subset \mathscr{C}$, which we will do by induction on n. The base case, that $F_0 = \mathbb{Q} \subset \mathscr{C}$, follows from the fact that $\mathscr{C}$ is a subfield of $\mathbb{C}$, whose prime subfield is $\mathbb{Q}$. For the inductive hypothesis, assume $F_{k-1} \subset \mathscr{C}$ for some $1 \leq k \leq n$. Recall that in characteristic 0, any quadratic extension is generated by the square root of some element in the base field. Thus, we can write $F_k = F_{k-1}(\sqrt{\gamma})$ for some $\gamma \in F_{k-1} \subset \mathscr{C}$. Then, by Theorem 1.3, $\sqrt{\gamma} \in \mathscr{C}$, and so $F_k \subset \mathscr{C}$.

Now, instead assume $\alpha \in \mathscr{C}$. Then, by definition, we can construct α from 0 and 1 in some number of steps s, where each step involves one of our five axioms. We will prove the theorem using induction on s. For the base case $s = 0$, α was constructed in zero steps, so it must be either 0 or 1. Then, $\alpha \in \mathbb{Q}$, so we can trivially take the required tower of extensions to just be $\mathbb{Q}$. Now, for the inductive hypothesis, suppose the required tower of extensions exists for any $\beta \in \mathbb{C}$ that can be constructed in $s-1$ steps. Let $\alpha \in \mathbb{C}$ be constructible in s steps.

Consider the final, s-th step of the construction of α: if it involved the construction of a line or a circle, it would be unnecessary, and so α could be constructed in $s-1$ steps. Then, by our inductive hypothesis, we would be done. Thus, assume the final step involves the intersection of either two lines, two circles, or a line and a circle. In any case, these lines/circles must have been constructed from four points (two each) $\beta_1, \beta_2, \beta_3, \beta_4$. In turn, each of these points must have been constructed in less than s steps, so by the inductive hypothesis, there exist extensions

$$F_n/F_{n-1}/\cdots/F_1/F_0 = \mathbb{Q},$$

where the degree of each extension is 2 and $\beta_1, \beta_2, \beta_3, \beta_4 \in F_n$. One can check that any lines and circles constructed from these points will be of the form

$$\begin{aligned} c_1x + c_2y &= c_3, \\ x^2 + y^2 + c_4x + c_5y &= c_6, \end{aligned}$$

where each c_i is also in F_n. Since these equations are at most degree 2, it follows that the solution (x, y) to any two such equations lies in some quadratic extension of F_n. These solutions correspond to intersections of the lines/circles, so in particular $\alpha = x + iy$ for some $x, y \in F_{n+1}$, where F_{n+1} is some quadratic extension of F_n. Then, $\alpha \in F_{n+1}(i)$, so we have extensions (excluding the top one if $i \in F_{n+1}$):

$$F_{n+1}(i)/F_{n+1}/F_n/\cdots/F_1/F_0 = \mathbb{Q},$$

where the degree of each extension is 2 and $\alpha \in F_{n+1}(i)$. □

Corollary 2.2. *$\mathscr{C}$ is the smallest subfield of $\mathbb{C}$ that is closed under taking square roots.*

Proof. Note that the argument from the first paragraph of the previous proof was not particular to the constructible numbers. What it really showed was that if we have extensions

$$F_n/F_{n-1}/\cdots/F_1/F_0 = \mathbb{Q},$$

where the degree of each extension is 2 and $\alpha \in F_n$, then α is a member of any subfield of $\mathbb{C}$ which is closed under taking square roots. But we showed we have such a tower of extensions exactly when α is constructible, and so every constructible number is a member of all subfields of $\mathbb{C}$ which are closed under taking square roots. Since we have already seen in Theorem 1.3 that $\mathscr{C}$ is closed under taking square roots, it follows that $\mathscr{C}$ is the smallest subfield of $\mathbb{C}$ that is closed under taking square roots. □

Corollary 2.3. *If $\alpha \in \mathscr{C}$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2. In other words, α is algebraic over $\mathbb{Q}$, and the degree of its minimal polynomial is a power of 2.*

Proof. By the theorem, we have extensions

$$F_n/F_{n-1}/\cdots/F_1/F_0 = \mathbb{Q},$$

where the degree of each extension is 2 and $\alpha \in F_n$. Therefore,

$$\big[F_n : \mathbb{Q}\big] = \big[F_n : F_{n-1}\big]\big[F_{n-1} : F_{n-2}\big]\cdots\big[F_1 : \mathbb{Q}\big] = 2^m,$$

for some $m \in \mathbb{N}$. Also, since $\alpha \in F_n$, we have extensions $F_n/\mathbb{Q}(\alpha)/\mathbb{Q}$, so

$$\big[F_n : \mathbb{Q}\big] = \big[F_n : \mathbb{Q}(\alpha)\big]\big[\mathbb{Q}(\alpha) : \mathbb{Q}\big].$$

It follows that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divides 2^m, and so $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is itself a power of 2. □

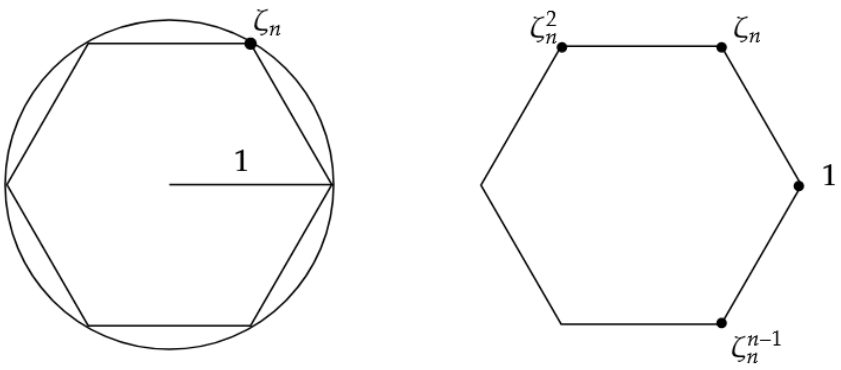
This result is enough to settle the questions raised at the beginning concerning whether it is possible to square a circle, trisect an angle, or duplicate a cube.

Example 2.4. *It is not possible to square a circle (to construct a square with equal area to a given circle) using a straight-edge and compass.*

Proof. Starting from a given circle, marking its center and any single point on its edge gives us two points, which we can call 0 and 1. Then, the radius of the circle is 1, so its area is π. If we were to construct a square with the same area, we would have to construct the length of its sides, $\sqrt{\pi}$, starting from 0 and 1. However, $\sqrt{\pi}$ is known to be transcendental over $\mathbb{Q}$, and so by Corollary 2.3, it is not constructible. □

Example 2.5. *It is not possible to trisect every angle using a straight-edge and compass.*

Proof. In Exercise 2.1, you will show it is possible to construct the angle $2\pi/3$ from 0 and 1. Thus, if we were able to trisect this angle, we would be able to construct the angle $2\pi/9$ from 0 and 1. Intersecting this angle with the unit circle would give us the ninth root of unity $\zeta_9 = e^{2\pi i/9}$. However, the minimal polynomial of ζ_9 over $\mathbb{Q}$ is $x^6 + x^3 + 1$, so by Corollary 2.3, it is not constructible. □



(a) (b)

Figure 3: (a) constructing ζ_n from a regular n-gon and (b) constructing a regular n-gon from ζ_n.

As we have seen, Corollary 2.3 is very useful for determining when a complex number is *not* constructible. However, it cannot be used to prove that a complex number is constructible, so we might wonder whether its converse is true. That is, we might wonder if $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ being a power of 2 is sufficient for α to be constructible. This turns out to be false in general, but using the following theorem we will prove it is true when $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois.

Theorem 2.6. *A complex number α is constructible if and only if $[L : \mathbb{Q}]$ is a power of 2, where L is the splitting field of the minimal polynomial of α over $\mathbb{Q}$.*

A proof of this, using the primitive element theorem and a result about solvable groups, can be found on page 263 of Cox.

Corollary 2.7. *If $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, then α is constructible if and only if $[\mathbb{Q}(\alpha)/\mathbb{Q}]$ is a power of 2.*

Proof. The forward direction follows from Corollary 2.3. For the other direction, assume $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2. Since $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, it is normal, so the minimal polynomial of α splits in $\mathbb{Q}(\alpha)$. Therefore, $\mathbb{Q}(\alpha)$ contains the splitting field L of this polynomial, giving us extensions $\mathbb{Q}(\alpha)/L/\mathbb{Q}$. It follows that

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : L][L : \mathbb{Q}].$$

Since $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2, $[L : \mathbb{Q}]$ must also be a power of 2, and so α is constructible by Theorem 2.6. □

This result allows us to prove the constructibility of a wide variety of numbers and shapes. For example, using properties of cyclotomic polynomials, we can determine all n for which a regular n-gon is constructible.

Theorem 2.8. *For any integer $n > 2$, a regular n-gon can be constructed if and only if $\phi(n)$ is a power of 2 (where ϕ is Euler's totient function). Equivalently, if and only if*

$$n = 2^s p_1 p_2 \cdots p_r,$$

for distinct Fermat primes $p_1, \ldots, p_r$.

Proof. As shown in Figure 3, a regular n-gon can be constructed if and only if a primitive n-th root of unity ζ_n can be constructed. It is known that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois (Cox, p. 201) and that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ (Cox, p. 235). Therefore, by Corollary 2.7, ζ_n is constructible if and only if $\phi(n)$ is a power of 2.

Now, factoring n as $n = 2^s p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are any distinct odd primes, we can use the following formula for Euler's totient function:

$$\phi(n) = 2^{s-1} p_1^{a_1-1}(p_1 - 1) \cdots p_r^{a_r-1}(p_r - 1).$$

We see this is a power of 2 exactly when $a_i = 1$ and $p_i = 2^{k_i} + 1$ for all i. However, primes of the form $2^k + 1$ are exactly the Fermat primes (k must itself be a power of 2), and so the theorem follows. □

Exercise 2.1. *Example 2.5 shows there are some angles which cannot be trisected using a straight-edge and compass. Some angles can be, however: use Theorem 2.1 to show the angle 2π can be trisected (i.e., that it is possible to construct $\zeta_3 = e^{2\pi i/3}$).*

Solution. Note that the minimal polynomial of ζ_3 over $\mathbb{Q}$ is x^2+x+1, so the extension $[\mathbb{Q}(\zeta_3) : \mathbb{Q}]$ has degree 2. Thus, we have the extension $\mathbb{Q}(\zeta_3)/\mathbb{Q}$, with degree 2, where $\zeta_3 \in \mathbb{Q}(\zeta_3)$. By Theorem 2.1, ζ_3 is constructible. □

Exercise 2.2. *Using Corollary 2.3, show it is not possible to duplicate a cube (to construct a cube with twice the volume of a given cube) using a straight-edge and compass.*

Solution. Starting from a given cube, marking two adjacent corners gives us two points, which we can call 0 and 1. Then, the volume of the cube is 1. If we were to construct a cube with twice the volume, we would have to construct the length of one of its sides, $\sqrt[3]{2}$, starting from 0 and 1. However, the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$, which has degree 3. Thus, by Corollary 2.3, $\sqrt[3]{2}$ is not constructible. □

3 Origami

We will now discuss an alternative method of construction: origami. This will turn out to be a more powerful method than ruler and compass, allowing us to trisect arbitrary angles and solve cubic equations.

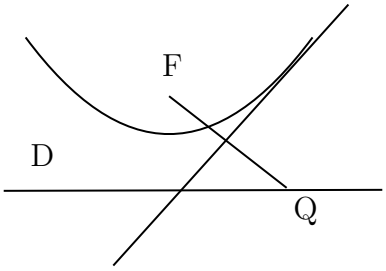
It will require us to define another construction rule, but first a quick note: for simplicity, all of the previously shown construction rules will apply while working with origami numbers. This seemingly implies the use of a ruler, compass, and paper folding, but it has been shown that all of the previous construction rules can be perfectly mimicked by origami alone, making the choice arbitrary. It will merely allow us to avoid slogging through the mechanics of actually performing the folds

with paper. We will now define the construction axiom which is to be added to the others:

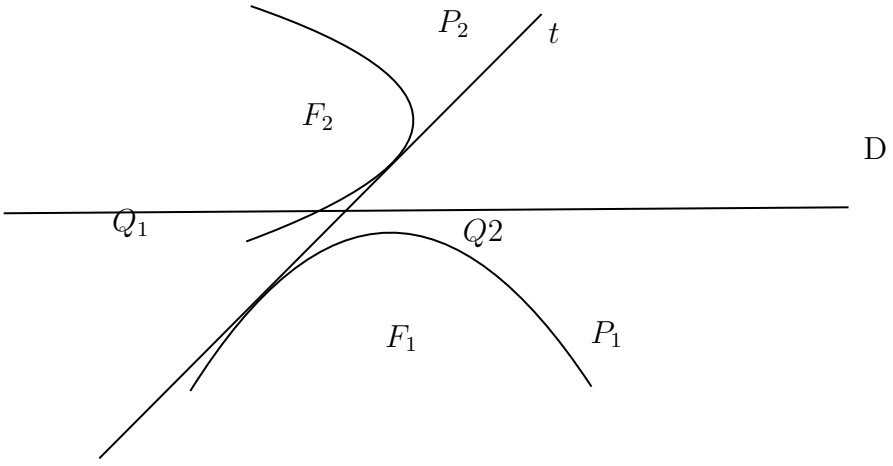
C3: Given two points, P and Q such that $P \neq Q$, and two lines, L_1 and L_2 such that $L_1 \neq L_2$, we can create the line L_3 that reflects P to L_1 and Q to L_2, if such a line exists.

Note that C3 only constructs the line L_3: in origami a line is a fold and point is the intersection of folds. However, the reflections of P and Q are trivially retrievable by straight edge and compass constructions. We thus define an origami number as a complex number that is the result of some finite combination of C3 and our original straight edge and compass constructions.

We will give an overview of how to solve cubic equations and trisect angles using origami. This will be a summary of the work of R. Geretschlager in [1]. Geretschlager shows that one can use origami to construct a tangent line by folding the focus to some point on the directrix.



Now suppose you are given two parabolas, each with a focus and a directrix, and suppose these parabolas have some common tangent. Continuous folding from f_1 to d_1 will eventually give us all of the tangents to p_1. If we move our fold that takes f_1 to d_1 along d_1 we will eventually reach a point in which f_2 is brought to d_2 as well. This line will then be our common tangent. Geretschlager shows that this line is constructible by origami.



Consider two parabolas:

$$p_1 : \quad (y-n)^2 = 2a(x-m),$$
$$p_2 : \quad x^2 = 2by.$$

Let the common tangent to these two parabolas be an arbitrary linear equation, $t : y = cx + d$, and let (x_1, y_1) be the point at which t is tangent to p_1. Using our equation for p_1 we can then express t as,

$$(y-n)(y_1-n) = a(x-m) + a(x_1-m).$$

Algebraic manipulation gives us the equivalent expression,

$$y = \frac{a}{y_1-n} \cdot x + n + \frac{ax_1 - 2am}{y_1-n}.$$

And so,

$$y_1 = \frac{a+nc}{c}$$
$$x_1 = \frac{d-n}{c} + 2m$$

Going back to our equation for p_1 and rearranging we wind up with,

$$a = 2c(d-n+cm) \tag{1}$$

Now, let (x_2, y_2) be the point at which t is tangent to p_2. Similarly to the above process we get the following equation for t,

$$y = \frac{x_2}{b} \cdot x - y_2,$$

which allows to find an expression for d,

$$d = -\frac{bc^2}{2}.$$

We then substitute this value for d into (1). The result post simplification is,

$$c^3 - \frac{2m}{b} \cdot c^2 + \frac{2n}{b} \cdot c + \frac{a}{b} = 0 \tag{2}$$

And so the slope of the common tangent is a solution to the above cubic equation. The upshot is that given a cubic equation all we need to do is construct the focus and directrix of p_1 and p_2 before we are able to fold the simultaneous tangent and solve the equation.

The ability to trisect an angle is a consequence of this result. Note the sin identity $\sin(3x) = 3\sin(x) - 4\sin^3(x)$. Given some angle θ we can find $\frac{\theta}{3}$ by solving the cubic equation $x^3 - \frac{3x}{4} + \frac{sin(\theta)}{4} = 0$.

Theorem 3.1. *The set of origami numbers is a subfield of $\mathbb{C}$ with the following characteristics:*

1. Let $\alpha = a + bi$ where $a, b \in \mathbb{R}$. Then, α is origami if and only if a and b are origami.

2. If α is origami then $\sqrt{\alpha}$ and $\sqrt[3]{\alpha}$ are origami.

3. α is origami if and only if there are subfields $\mathbb{Q} = F_0 \subset ... \subset F_n \subset \mathbb{C}$ such that $\alpha \in F_n$ and $[F_i : F_{i-1}] = 2$ or 3 for $1 \leq i \leq n$.

Proof. The proof that the origami numbers constitute a field will follow once an identical result is proven for conics later in the paper. Part (a) will be omitted as it mirrors the proof of Theorem 1.1.

For part (b) it will be useful to work in polar coordinates. Let $\alpha = re^{i\theta}$. By inheriting straight edge and compass constructions we have instantly that $\sqrt{r}$ is origami. We are also able to bisect θ. It follows that $\sqrt{\alpha}$ will be origami. For the cube root, recall that we can trisect an arbitrary angle. To construct $\sqrt[3]{r}$ we will make use of the ability of origami to construct simultaneous tangents. Consider the parabolas $(y = (1/2)(a))^2 = 2bx$ and $y = (1/2)x^2$. We are able to build the foci and directrices by ruler and compass and then the simultaneous tangent by origami. Simple algebra shows that the slope of this tangent is $\sqrt[3]{r}$, which implies that $\sqrt[3]{r}$ is origami and therefore $\sqrt[3]{\alpha}$ is also origami.

Finally, part (c). Begin by supposing we have such a 2-3 tower. Our goal is to show that $F_n \subset O$, where O is the set of all origami numbers. We will give an inductive argument. Note that the $n = 0$ case is trivial and then assume that $F_{n-1} \subset O$. Take some $\alpha \in F_n$. Due to the fact that $[F_n : F_{n-1}] = 2$ or 3 we have that alpha is the root of some polynomial of degree at most 3 with origami coefficients. By cases, if the polynomial is degree 1, clearly α will be origami. If the degree is 2 or 3 we can express α as some combination of square roots, cube roots, and other origami numbers, and by part (b) this implies that α is origami.

For the next direction of part (c) we will leverage part (a), namely that for some $\alpha = a + bi$ if a and b are origami then α is as well. Therefore our goal will be to show the existence of a 2-3 tower such that F_n contains the real and imaginary parts of every origami number used in the construction of α. This is the same strategy as was used to prove Theorem 2.1 and will therefore be omitted. □

The book gives the following example of part (c):

Example 3.2. *The 2-3 tower $\mathbb{Q} \subset \mathbb{Q}(2cos(2\pi/7)) \subset \mathbb{Q}(\xi_7)$ shows that ξ_7 is origami. It follows that a regular 7-gon is constructible.*

We give this example to foreshadow a result coming later: a complete characterization of n-gons constructible with origami.

Theorem 3.3. *Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$ and let $\mathbb{Q} \subset L$ be the splitting field of the minimal polynomial of α over $\mathbb{Q}$. Then α is an origami number if and only if*

$[L : \mathbb{Q}] = 2^a 3^b$ *for some integers* $a, b \geq 0$.

We will prove an equivalent theorem in the language of conics. Since the set of origami numbers is the same as the set of conic constructible numbers this result will follow.

4 Conics

There is another method of construction that turns out to be equivalent to origami: intersecting conics. This section is entirely a retelling of the work done by Carlos Videla in [2].

We define conics as a curve in the plane given by equations of the form:

$$F(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0 \tag{3}$$

where $a, b, c, d, e, f \in \mathbb{R}$ and a, b, c are nonzero. We also restrict ourselves to equations with at least one solution with $x, y \in \mathbb{R}$. We will prove equivalence between the set of conic constructed numbers and origami numbers, use this equivalence to prove facts about origami, and characterize the n-gons that are able to be constructed by conics (and as a result, origami).

Theorem 4.1. *The set of conic constructible points,* C*, is a subset of* $\mathbb{C}$ *that is closed under conjugation, square roots, and cube roots, and is the smallest such subset.*

Proof. We start by taking an arbitrary $C' \in \mathbb{C}$ which is closed under conjugation, square roots, and cube roots. Our strategy will be to construct conics using points in C' and lengths between points in C' and then show that the intersection of such conics results in points in C'.

Recall that if $\alpha = a + bi \in C'$ then $a, b \in C'$ and vice versa. Then, if we build our conic out of points from C', it's equation will have coefficients in C'. If we intersect two distinct conics we will get a maximum of 4 points. To find the coordinates of these points we solve the equations for our conics simultaneously. The result will lead us to having a polynomial, $P(x)$ or $Q(y)$ depending, with a maximal degree of 4 and real coefficients in C' that equals 0. From earlier results with regards to ruler and compass constructions the roots of these polynomials are obtained by taking square and cube roots of elements of C'. If the result of this process is the $x-$coordinates of the intersections then we may solve for the $y-$coordinates using the quadratic formula, and so if $x + yi$ is a point of intersection it is in C'.

What is left is to check that we can actually construct $P(x)$ and $Q(y)$. Looking back to our equation for conics the construction is straight forward, except for the xy term. We will split it into three cases: either $b = b' = 0$, $b \neq 0$ and $b' \neq 0$, or $b = 0$ and $b' \neq 0$. The first case is trivial. The second case reduces to the third by way of scaling one of the polynomials and subtracting such that the xy term cancels in one of them. We now approach the final case in which one conic, E, has an xy term and the other, E' does not.

We can translate our conics using ruler and compass constructions such that $E \to E*$ and $E' \to E*'$ and $E*'$ is centered at the origin. We can consider three cases, which cover all possible forms for $E*'$: a parabola, a circle or ellipse, or a hyperbola.

1. $E*'$ is a parabola. If so, without loss of generality, $E*' : y = mx^2 + b$ where $a, b \in C' \cap \mathbb{R}$. After substitution of the equation for $E*$ we see that either $P(x) = 0$ or $Q(y) = 0$ with a maximal degree of 4. This tells us that the intersection of our translated conics is in C', and it follows that our original conics are in C' as well, as desired.

2. $E*'$ is a circle. Then, $E*'$ follows the equation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ where $a, b \in C' \cap \mathbb{R}$. Solving for x^2 and substituting into the equation for $E*$ gives the result after a bit of algebraic manipulation.

3. The final case where where $E*'$ is a hyperbola is handled identically to case (2). This finishes the proof. □

Now, we will prove the following result.

Theorem 4.2. *Let $z \in \mathbb{C}$ be given. Then z is conic constructible if and only if z is contained in a subfield of $\mathbb{C}$ of the form $\mathbb{Q}(\alpha_1, ...\alpha_l)$ where $\alpha_1^n \in \mathbb{Q}$ and $\alpha_i^n \in \mathbb{Q}(\alpha_1, ...\alpha_i - 1)$ for $2 \leq i \leq l$ and $n \in [2, 3]$.*

Proof. Our goal is to show an equivalence between the set of conic constructible numbers, C, and the set of complex numbers that live in such a $(2-3)$ tower, C'. By the previous theorem we have that C is closed under square and cube roots. It follows that $C' \subset C$. For the other inclusion note that $\overline{\mathbb{Q}(\alpha_1, ...\alpha_l)} = \mathbb{Q}(\overline{\alpha_1}, ..., \overline{\alpha_l})$. Then, since C' is closed under square and cube roots, it is closed under conjugation, and we have $C \subset C'$, completing the proof. □

We can combine Theorem 4.2 with part (3) of Theorem 3.1 to gain an immediate result.

Theorem 4.3. *Let $\alpha \in \mathbb{C}$. Then α is conic constructible if and only if α is an origami number.*

Theorem 4.4. *A complex number z is conic constructible if and only if z is algebraic over $\mathbb{Q}$ and the normal closure of $K/\mathbb{Q}$ of $\mathbb{Q}(z)/\mathbb{Q}$ has dimension $2^n 3^m$ over $\mathbb{Q}$ where $n, m \in \mathbb{N}$.*

First, we will prove the following lemma from [3].

Lemma 4.5. *Let E/F have a root tower over F, $F = F_1 \subset F_{r+1} = E$ where $F_{i+1} = F_i(d_i)$ with $d_i^{n_i} \in F_i$. Assume that E is generated over F by a finite set of elements whose minimum polynomials are separable. Then the normal closure K/F of E/F has a root tower over F such that the distinct integers n_i for this tower are the same as those occurring in the given tower.*

Proof of lemma. Let $\eta(E)$, $\eta \in \mathrm{Gal}K/F$ be the conjugate field which generates the normal closure K/F. If we apply η to the described tower F the result is a root tower

for $\eta(E)$ over F.Then, $K = F(\eta_1(d_1), ..., \eta_1(d_r); \eta_2(d_1), ..., \eta_2(d_r); ...)$. We have such a root tower for K over F satisfying the conditions, which shows the lemma. □

Proof of theorem. Assume that z is conic constructible. It follows by Theorem 4.2 that z is contained in a $(2-3)$ tower. By the lemma we are able to assume that this tower is Galois. This tells us the dimension of the normal closure $K/\mathbb{Q}$ of $\mathbb{Q}/z/\mathbb{Q}$ over $\mathbb{Q}$: 2^n3^m. Note that $K/\mathbb{Q}$ is a subfield of $\mathbb{Q}(\alpha_1, ...\alpha_l)$.

In the other direction, suppose the normal closure $K/\mathbb{Q}$ of $\mathbb{Q}(z)/\mathbb{Q}$ has dimension 2^s3^t over $\mathbb{Q}$. Then G =Gal$(K/\mathbb{Q})$ has order 2^s3^t. We now apply Burnside's Theorem (8.1.8, Cox), which states if a finite group is of order p^ap^b where p, q are prime and a, b are non-negative integers then the group is solvable, to get that G is solvable. It follows from this that G has a composition series $G = G_1 \triangleright G_2... \triangleright G_k = 1$ such that G_i/G_{i+1} is of order 2 or 3. Applying the main theorem of Galois Theory we have the following collection of subfields: $\mathbb{Q} = F_1 \subset ... \subset F_l = K$. We know that $[F_{i+1} : F_i] =$ 2 or 3. Denote $F_{i+1} = F_i(\alpha_i)$. If the extension is degree 2 it comes from adjoining a square root. If the extension is of degree 3 and does not come from adjoining a cube root then we can construct the following sequence: $f_i \subset L_i' \subset L_i'' \subset L_i'''$ where $\alpha_i \in L_i'''$. This is a $(2-3)$ tower can be used in place of the tower at the ith extension $F_i \subset F_{i+1}$. It follows that z lives in a $(2-3)$ tower and thus by Theorem 4.2 is conic constructible. □

We are now able to characterize which polygons are conic constructible (or equivalently, origami constructible).

Theorem 4.6. *A regular n-sided polygon is conic constructible if and only if* $n = 2^s3^tp_1, ..., p_s$ *where* $a, b \geq 0$ *and* $p_1, ..., p_s$ *are distinct Pierpont primes (primes of the form* $2^k3^l + 1$*).*

The proof of this theorem is very similar to that of Theorem 2.8, and is omitted.

References

[1] R. Geretschlager, Euclidean Constructions and the Geometry of Origami, Taylor and Francis, 1995.

[2] C. R. Videla, On Points Constructible from Conics, Math Intelligencer, no. 2, 1997.

[3] N. Jacobson, Basic Algebra I, W.H. Freeman and Co., New York, 1985.

[4] D. Cox, Galois Theory, John Wiley and Sons, 2021.