Geometric constructions in relation with algebraic and transcendental numbers

Jean-Pierre Demailly

Académie des Sciences de Paris, and
Institut Fourier, Université de Grenoble I, France

February 26, 2010 / Euromath 2010 / Bad Goisern, Austria

Ruler and compasses vs. origamis

Ancient Greek mathematicians have greatly developed geometry (Euclid, Pythagoras, Thales, Eratosthenes...)

Ruler and compasses vs. origamis

Ancient Greek mathematicians have greatly developed geometry (Euclid, Pythagoras, Thales, Eratosthenes...)

They raised the question whether certain constructions can be made by ruler and compasses

Ruler and compasses vs. origamis

Ancient Greek mathematicians have greatly developed geometry (Euclid, Pythagoras, Thales, Eratosthenes...)

They raised the question whether certain constructions can be made by ruler and compasses

Quadrature of the circle ? This means: constructing a square whose perimeter is equal to the perimeter of a given circle. It was solved only in 1882 by Lindemann, after more than 2000 years : construction is not possible with ruler and compasses !

Ruler and compasses vs. origamis

Ancient Greek mathematicians have greatly developed geometry (Euclid, Pythagoras, Thales, Eratosthenes...)

They raised the question whether certain constructions can be made by ruler and compasses

Quadrature of the circle ? This means: constructing a square whose perimeter is equal to the perimeter of a given circle. It was solved only in 1882 by Lindemann, after more than 2000 years : construction is not possible with ruler and compasses !

Neither is it possible to trisect an angle (Wantzel 1837)

Ruler and compasses vs. origamis

Ancient Greek mathematicians have greatly developed geometry (Euclid, Pythagoras, Thales, Eratosthenes...)

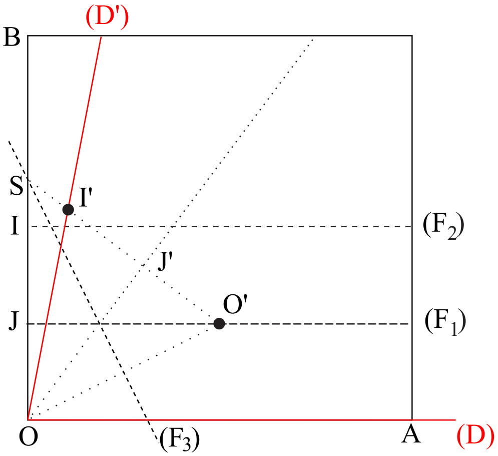
They raised the question whether certain constructions can be made by ruler and compasses

Quadrature of the circle ? This means: constructing a square whose perimeter is equal to the perimeter of a given circle. It was solved only in 1882 by Lindemann, after more than 2000 years : construction is not possible with ruler and compasses !

Neither is it possible to trisect an angle (Wantzel 1837)

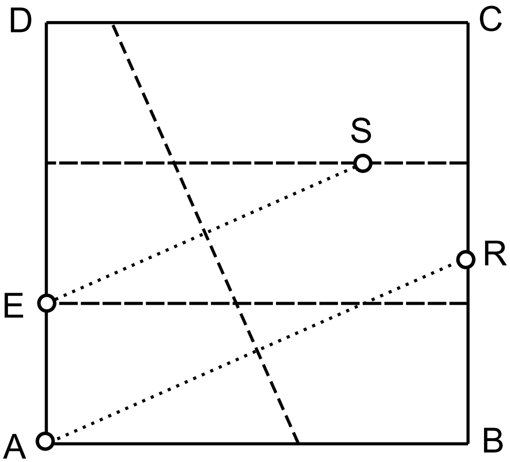
In Japan, on the other hand, there is a rich tradition of making origamis : it is the art of folding paper and maker nice geometric constructions out of such foldings.

Trisection of an angle with origamis



Folding along $(F3)$ so that O is brought to $O' \in (F_1)$ and I is brought to $I' \in D'$ constructs the trisection of angle(D, D') !

Cube root of 2 with origamis



Exercise. Show that this construction can be used to produce $\sqrt[3]{2}$ (side of the square is 3).

“Axioms” for ruler and compasses

- One starts from a given set of points S
  (quit often just two points $S = \{O, A\}$)
  Then enlarge S into $S' \supset S$ by constructing lines and circles according to the following rules:

“Axioms” for ruler and compasses

- One starts from a given set of points S
  (quit often just two points $\mathrm{S} = \{\mathrm{O}, \mathrm{A}\}$)
  Then enlarge S into $\mathrm{S}' \supset \mathrm{S}$ by constructing lines and circles according to the following rules:
- Axiom (RC1). Given two points M, N already constructed in S', one can construct the line (MN) or the circle of center M passing through N (or vice versa).

"Axioms" for ruler and compasses

- One starts from a given set of points S
  (quit often just two points $\mathrm{S} = \{\mathrm{O}, \mathrm{A}\}$)
  Then enlarge S into $\mathrm{S}' \supset \mathrm{S}$ by constructing lines and circles according to the following rules:
- Axiom (RC1). Given two points M, N already constructed in S', one can construct the line (MN) or the circle of center M passing through N (or vice versa).
- Axiom (RC2). Given 2 lines, 1 line and a circle, or 2 circles constructed from RC1, S' contains all points of intersection of these.

“Axioms” for ruler and compasses

- One starts from a given set of points S
  (quit often just two points $\mathrm{S} = \{\mathrm{O}, \mathrm{A}\}$)
  Then enlarge S into $\mathrm{S}' \supset \mathrm{S}$ by constructing lines and circles according to the following rules:
- Axiom (RC1). Given two points M, N already constructed in S', one can construct the line (MN) or the circle of center M passing through N (or vice versa).
- Axiom (RC2). Given 2 lines, 1 line and a circle, or 2 circles constructed from RC1, S' contains all points of intersection of these.
- Question : Describe the set of points $\mathrm{Constr}_{\mathrm{RC}}(\mathrm{S})$ which can be constructed from S in finitely many steps.

Complex numbers

- One introduces the "imaginary number" denoted $\mathrm{i} = \sqrt{-1}$ which does not exist among real numbers ($x^2 = -1$ has no solution in $\mathbb{R}$)

Complex numbers

- One introduces the “imaginary number” denoted $i = \sqrt{-1}$ which does not exist among real numbers ($x^2 = -1$ has no solution in $\mathbb{R}$)
- Complex numbers are combinations $x + iy$ where x, y are real numbers, e.g. $2 + 3i$. Their set is denoted $\mathbb{C}$.

Complex numbers

- One introduces the "imaginary number" denoted $i = \sqrt{-1}$ which does not exist among real numbers ($x^2 = -1$ has no solution in $\mathbb{R}$)
- Complex numbers are combinations $x + iy$ where x, y are real numbers, e.g. $2 + 3i$. Their set is denoted $\mathbb{C}$.
- Addition in $\mathbb{C}$

$$(x + iy) + (x' + iy') = (x + x') + i(y + y'),$$

e.g. $(2 + 3i) + (-7 + 8i) = -5 + 11i$

Complex numbers

- One introduces the "imaginary number" denoted $i = \sqrt{-1}$ which does not exist among real numbers ($x^2 = -1$ has no solution in $\mathbb{R}$)
- Complex numbers are combinations $x + iy$ where x, y are real numbers, e.g. $2 + 3i$. Their set is denoted $\mathbb{C}$.
- Addition in $\mathbb{C}$

$$(x + iy) + (x' + iy') = (x + x') + i(y + y'),$$

e.g. $(2 + 3i) + (-7 + 8i) = -5 + 11i$

- Multiplication in $\mathbb{C}$

$$\begin{aligned}(x + iy) \times (x' + iy') &= xx' + ixy' + iyx' + i \times i \times yy' \\ &= xx' + ixy' + iyx' + (-1) \times yy' \\ &= (xx' - yy') + i(xy' + yx')\end{aligned}$$

Geometric interpretation of complex numbers

- Complex numbers are identified with points of a euclidean plane, once one chooses an origin O and a point A representing 1

Geometric interpretation of complex numbers

- Complex numbers are identified with points of a euclidean plane, once one chooses an origin O and a point A representing 1
- Interpretation of addition in $\mathbb{C}$ Addition corresponds to adding vectors in the plane: use a parallelogram

Geometric interpretation of complex numbers

- Complex numbers are identified with points of a euclidean plane, once one chooses an origin O and a point A representing 1
- Interpretation of addition in $\mathbb{C}$ Addition corresponds to adding vectors in the plane: use a parallelogram
- Interpretation of multiplication in $\mathbb{C}$ Introduce $|\mathrm{z}| = \sqrt{\mathrm{x}^2 + \mathrm{y}^2}$ and $\arg(\mathrm{z}) = \mathrm{angle}(0\mathrm{x}, \mathrm{Oz})$. Then

$$|\mathrm{zz}'| = |\mathrm{z}|\ |\mathrm{z}'|, \qquad \arg(\mathrm{zz}') = \arg(\mathrm{z}) + \arg(\mathrm{z}') \mod 2\pi$$

Square roots always exist in $\mathbb{C}$!

- $\sqrt{-x} = \pm i\sqrt{x}$ if x is a positive real number.

Square roots always exist in $\mathbb{C}$!

- $\sqrt{-x} = \pm i\sqrt{x}$ if x is a positive real number.
- Square root of a complex number: if $z = x + iy$, then

$$\sqrt{z} = \pm\Big(\sqrt{\frac{x+\sqrt{x^2+y^2}}{2}} + \varepsilon i\sqrt{\frac{-x+\sqrt{x^2+y^2}}{2}}\Big)$$

where $\varepsilon = +1$ if $y \geq 0$ and $\varepsilon = -1$ if $y < 0$.

Square roots always exist in $\mathbb{C}$!

- $\sqrt{-x} = \pm i\sqrt{x}$ if x is a positive real number.
- Square root of a complex number: if $z = x + iy$, then

$$\sqrt{z} = \pm\left(\sqrt{\frac{x+\sqrt{x^2+y^2}}{2}} + \varepsilon i\sqrt{\frac{-x+\sqrt{x^2+y^2}}{2}}\right)$$

  where $\varepsilon = +1$ if $y \geq 0$ and $\varepsilon = -1$ if $y < 0$.
- Theorem (d'Alembert-Gauss) Every polynomial of degree d $a_d z^d + a_{d-1} z^{d-1} + \ldots + a_1 z + a_0$ with coefficients in $\mathbb{C}$ has exactly d roots when counted with multiciplicities.

Square roots always exist in $\mathbb{C}$!

- $\sqrt{-x} = \pm i\sqrt{x}$ if x is a positive real number.
- Square root of a complex number: if $z = x + iy$, then

$$\sqrt{z} = \pm\left(\sqrt{\frac{x+\sqrt{x^2+y^2}}{2}} + \varepsilon i\sqrt{\frac{-x+\sqrt{x^2+y^2}}{2}}\right)$$

  where $\varepsilon = +1$ if $y \geq 0$ and $\varepsilon = -1$ if $y < 0$.

- Theorem (d'Alembert-Gauss) Every polynomial of degree d $a_d z^d + a_{d-1} z^{d-1} + \ldots + a_1 z + a_0$ with coefficients in $\mathbb{C}$ has exactly d roots when counted with multiciplicities.
- Definition One says that $z \in \mathbb{C}$ is an algebraic number if it is a solution of a polynomial with $a_j \in \mathbb{Q}$ (or $a_j \in \mathbb{Z}$), a transcendental number otherwise

Example of algebraic and transcendental numbers

- Although irrational, $z = \sqrt{2}$ is algebraic since $z^2 - 2 = 0$.

Example of algebraic and transcendental numbers

- Although irrational, $z = \sqrt{2}$ is algebraic since $z^2 - 2 = 0$.
- $z = i\sqrt{2}$ is also algebraic since $z^2 + 2 = 0$.

Example of algebraic and transcendental numbers

- Although irrational, $z = \sqrt{2}$ is algebraic since $z^2 - 2 = 0$.
- $z = i\sqrt{2}$ is also algebraic since $z^2 + 2 = 0$.
- Hermite (1872): $e = \exp(1)$ is transcendental.

Example of algebraic and transcendental numbers

- Although irrational, $z = \sqrt{2}$ is algebraic since $z^2 - 2 = 0$.
- $z = i\sqrt{2}$ is also algebraic since $z^2 + 2 = 0$.
- Hermite (1872): $e = \exp(1)$ is transcendental.
- Lindemann (1882): π is transcendental.
  In fact if α is algebraic and non zero, then
  e^α is transcendental (Lindemann-Weierstrass 1885).
  Now π cannot be algebraic since $e^{i\pi} = -1$ is algebraic !

Example of algebraic and transcendental numbers

- Although irrational, $z = \sqrt{2}$ is algebraic since $z^2 - 2 = 0$.
- $z = i\sqrt{2}$ is also algebraic since $z^2 + 2 = 0$.
- Hermite (1872): $e = \exp(1)$ is transcendental.
- Lindemann (1882): π is transcendental.
  In fact if α is algebraic and non zero, then
  e^α is transcendental (Lindemann-Weierstrass 1885).
  Now π cannot be algebraic since $e^{i\pi} = -1$ is algebraic !
- Gelfond / Schneider (1934): if α and β are algebraic,
  $\alpha \neq 0, 1$ and $\beta \notin \mathbb{Q}$, then α^β is transcendental.
  For example, $2^{\sqrt{2}}$ is transcendental, as well as
  $e^\pi = (e^{i\pi})^{-i} = (-1)^{-i}$.

Example of algebraic and transcendental numbers

- Although irrational, $z = \sqrt{2}$ is algebraic since $z^2 - 2 = 0$.
- $z = i\sqrt{2}$ is also algebraic since $z^2 + 2 = 0$.
- Hermite (1872): $e = \exp(1)$ is transcendental.
- Lindemann (1882): π is transcendental.
  In fact if α is algebraic and non zero, then
  e^α is transcendental (Lindemann-Weierstrass 1885).
  Now π cannot be algebraic since $e^{i\pi} = -1$ is algebraic !
- Gelfond / Schneider (1934): if α and β are algebraic,
  $\alpha \neq 0, 1$ and $\beta \notin \mathbb{Q}$, then α^β is transcendental.
  For example, $2^{\sqrt{2}}$ is transcendental, as well as
  $e^\pi = (e^{i\pi})^{-i} = (-1)^{-i}$.
- Unknown whether e/π is transcendental, not even known that $e/\pi \notin \mathbb{Q}$!

Subfields of the field of complex numbers

- A subset $\mathbb{F} \subset \mathbb{C}$ is called a field (but there is a more general concept than just for numbers...) if $\mathbb{F}$ contains $0, 1$, and is stable by addition, subtraction, multiplication and division, (i.e. for $z, w \in \mathbb{F}$, we have $z + w \in \mathbb{F}$, $z - w \in \mathbb{F}$, $zw \in \mathbb{F}$, $z/w \in \mathbb{F}$ if $w \neq 0$)

Subfields of the field of complex numbers

- A subset $\mathbb{F} \subset \mathbb{C}$ is called a field (but there is a more general concept than just for numbers...) if $\mathbb{F}$ contains $0, 1$, and is stable by addition, subtraction, multiplication and division, (i.e. for $z, w \in \mathbb{F}$, we have $z + w \in \mathbb{F}$, $z - w \in \mathbb{F}$, $zw \in \mathbb{F}$, $z/w \in \mathbb{F}$ if $w \neq 0$)
- If $\mathbb{F}$ contains $0, 1, -1$, it is enough for $\mathbb{F}$ to be stable by addition, multiplication and especially inverse ($z \in \mathbb{F}$, $z \neq 0 \Rightarrow 1/z \in \mathbb{F}$).

Subfields of the field of complex numbers

- A subset $\mathbb{F} \subset \mathbb{C}$ is called a field (but there is a more general concept than just for numbers...) if $\mathbb{F}$ contains $0, 1$, and is stable by addition, subtraction, multiplication and division, (i.e. for $z, w \in \mathbb{F}$, we have $z + w \in \mathbb{F}$, $z - w \in \mathbb{F}$, $zw \in \mathbb{F}$, $z/w \in \mathbb{F}$ if $w \neq 0$)
- If $\mathbb{F}$ contains $0, 1, -1$, it is enough for $\mathbb{F}$ to be stable by addition, multiplication and especially inverse ($z \in \mathbb{F}$, $z \neq 0 \Rightarrow 1/z \in \mathbb{F}$).
- For example, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields but $\mathbb{Z}$ is not ($2 \in \mathbb{Z}$ but $1/2 \notin \mathbb{Z}$), nor is the set $\mathbb{D}$ of decimal numbers

Subfields of the field of complex numbers

- A subset $\mathbb{F} \subset \mathbb{C}$ is called a field (but there is a more general concept than just for numbers...) if $\mathbb{F}$ contains $0, 1$, and is stable by addition, subtraction, multiplication and division, (i.e. for $z, w \in \mathbb{F}$, we have $z + w \in \mathbb{F}$, $z - w \in \mathbb{F}$, $zw \in \mathbb{F}$, $z/w \in \mathbb{F}$ if $w \neq 0$)
- If $\mathbb{F}$ contains $0, 1, -1$, it is enough for $\mathbb{F}$ to be stable by addition, multiplication and especially inverse ($z \in \mathbb{F}$, $z \neq 0 \Rightarrow 1/z \in \mathbb{F}$).
- For example, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields but $\mathbb{Z}$ is not ($2 \in \mathbb{Z}$ but $1/2 \notin \mathbb{Z}$), nor is the set $\mathbb{D}$ of decimal numbers
- The set denoted $\mathbb{Q}[\sqrt{2}]$ of numbers of the form $x + y\sqrt{2}$, $x, y \in \mathbb{Q}$ is a field :
$$(x + y\sqrt{2})^{-1} = \frac{x - y\sqrt{2}}{x^2 - 2y^2} = \frac{x}{x^2 - 2y^2} - \frac{y}{x^2 - 2y^2}\sqrt{2}$$

Algebraic number fields

- Similarly the set denoted $\mathbb{Q}[\sqrt{-2}]$ of numbers of the form $x + y\sqrt{-2} = x + iy\sqrt{2}$, $x, y \in \mathbb{Q}$ is a field (exercise !)
  These fields are called quadratic fields

Algebraic number fields

- Similarly the set denoted $\mathbb{Q}[\sqrt{-2}]$ of numbers of the form $x + y\sqrt{-2} = x + iy\sqrt{2}$, $x, y \in \mathbb{Q}$ is a field (exercise !)
These fields are called quadratic fields
- The set $\mathbb{Q}[\sqrt[3]{2}]$ of numbers of the form $x + y\sqrt[3]{2} + z(\sqrt[3]{2})^2$, $x, y, z \in \mathbb{Q}$ is a field (cubic field)
This is a bit harder to prove.
Hint: calculate ω^3 where $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, and then show that the product

$$(x + y\omega\sqrt[3]{2} + z(\omega\sqrt[3]{2})^2)(x + y\omega^2\sqrt[3]{2} + z(\omega^2\sqrt[3]{2})^2)$$

no longer involves ω and yields a rational number when multiplied by $x + y\sqrt[3]{2} + z(\sqrt[3]{2})^2$.

Degree of a number field

- One can show (but this is yet harder) that if α, β, $\gamma, \ldots$ are algebraic numbers, then the sets $\mathbb{Q}[\alpha]$, $\mathbb{Q}[\alpha, \beta]$, $\mathbb{Q}[\alpha, \beta, \gamma]$ of polynomials $P(\alpha)$, $P(\alpha, \beta)$, $P(\alpha, \beta, \gamma)$ (...) with rational coefficients are fields.

Degree of a number field

- One can show (but this is yet harder) that if α, β, $\gamma, \ldots$ are algebraic numbers, then the sets $\mathbb{Q}[\alpha]$, $\mathbb{Q}[\alpha, \beta]$, $\mathbb{Q}[\alpha, \beta, \gamma]$ of polynomials $P(\alpha)$, $P(\alpha, \beta)$, $P(\alpha, \beta, \gamma)$ (...) with rational coefficients are fields.
- If $\mathbb{F} \subset \mathbb{G}$ are fields and every element $y \in \mathbb{G}$ can be written in a unique way $y = x_1\alpha_1 + \ldots + x_p\alpha_p$ for $x_i \in \mathbb{F}$ and certain (well chosen) elements $\alpha_i \in \mathbb{G}$, one says that $\mathbb{G}$ has (finite) degree p over $\mathbb{F}$, with basis (α_j) over $\mathbb{F}$, and one writes $[\mathbb{G} : \mathbb{F}] = p$

Degree of a number field

- One can show (but this is yet harder) that if $\alpha, \beta, \gamma, \ldots$ are algebraic numbers, then the sets $\mathbb{Q}[\alpha]$, $\mathbb{Q}[\alpha, \beta]$, $\mathbb{Q}[\alpha, \beta, \gamma]$ of polynomials $P(\alpha)$, $P(\alpha, \beta)$, $P(\alpha, \beta, \gamma)$ (...) with rational coefficients are fields.

- If $\mathbb{F} \subset \mathbb{G}$ are fields and every element $y \in \mathbb{G}$ can be written in a unique way $y = x_1\alpha_1 + \ldots + x_p\alpha_p$ for $x_i \in \mathbb{F}$ and certain (well chosen) elements $\alpha_i \in \mathbb{G}$, one says that $\mathbb{G}$ has (finite) degree p over $\mathbb{F}$, with basis (α_j) over $\mathbb{F}$, and one writes $[\mathbb{G} : \mathbb{F}] = p$

- Example: $[\mathbb{Q}[\sqrt[2]{:}\mathbb{Q}] = 2$ and $[\mathbb{Q}[\sqrt[3]{2} : \mathbb{Q}] = 3$.
- Exercise. If $\mathbb{G} = \mathbb{F}[\alpha]$ where $\alpha \in \mathbb{G}$, $\alpha \notin \mathbb{F}$ and α satisfies an equation of degree 2 with coefficients in $\mathbb{F}$, then $[\mathbb{G} : \mathbb{F}] = 2$. Idem for degree d if α does not satisfy any equation of lower order (take $\alpha_j = \alpha^j$, $0 \leq j \leq d-1$).

Successive extensions of fields

- **Theorem.** If $\mathbb{F} \subset \mathbb{G} \subset \mathbb{K}$ are fields then

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{G}] \times [\mathbb{G} : \mathbb{F}]$$

  if the degrees are finite.

Successive extensions of fields

- Theorem. If $\mathbb{F} \subset \mathbb{G} \subset \mathbb{K}$ are fields then
$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{G}] \times [\mathbb{G} : \mathbb{F}]$$
  if the degrees are finite.

- Proof. Write $p = [\mathbb{G} : \mathbb{F}]$ and $q = [\mathbb{K} : \mathbb{G}]$.
  Every $z \in \mathbb{K}$ can be written in a unique way
  $z = \sum_k y_k \beta_k, \quad y_k \in \mathbb{G}$ for a basis $\beta_1, \ldots, \beta_q \in \mathbb{K}$,
  and each $y_k \in \mathbb{G}$ can then be written in a unique way
  $y_k = \sum_j x_{jk} \alpha_j, \quad x_{jk} \in \mathbb{F}$ for a basis $\alpha_1, \ldots, \alpha_p \in \mathbb{G}$,
  so, uniquely in terms of the $\alpha_j \beta_k$ (check it!)
  $z = \sum_{j,k} x_{jk} \alpha_j \beta_k$.
  Thus $(\alpha_j \beta_k)$ is a basis of $\mathbb{K}$ over $\mathbb{F}$ and $[\mathbb{K} : \mathbb{F}] = pq$.

Re-interpretation of constructions with ruler and compasses

- We start from a set of points S in the plane (of at least two points) and interpret them as complex numbers in coordinates. By a rotation, change of origin and change of unit, we mant assume that two of these numbers are $s_1 = 0$, $s_2 = 1$, the other ones are complex numbers $s_3 \ldots, s_n$, $n = \sharp S$.

Re-interpretation of constructions with ruler and compasses

- We start from a set of points S in the plane (of at least two points) and interpret them as complex numbers in coordinates. By a rotation, change of origin and change of unit, we mant assume that two of these numbers are $s_1 = 0$, $s_2 = 1$, the other ones are complex numbers $s_3 \ldots, s_n$, $n = \sharp S$.
- Basic observation. The set of points constructible from S by ruler and compasses is stable by addition, multiplication, inverse, and also by conjugation and square root.

Re-interpretation of constructions with ruler and compasses

- We start from a set of points S in the plane (of at least two points) and interpret them as complex numbers in coordinates. By a rotation, change of origin and change of unit, we mant assume that two of these numbers are $s_1 = 0$, $s_2 = 1$, the other ones are complex numbers $s_3 \ldots, s_n$, $n = \sharp S$.
- Basic observation. The set of points constructible from S by ruler and compasses is stable by addition, multiplication, inverse, and also by conjugation and square root.
- The set $\mathbb{Q}(S)$ of all rational fractions $P(s_3, \ldots, s_n)/Q(s_3, \ldots, s_n)$ is a field (equal to $\mathbb{Q}$ if we start from only two points).

Necessary and sufficient condition for constructibility

- When we construct a bigger set $S' \subset S$ with ruler and compasses, we only solve linear and quadratic equations (intersections of lines and/or circles) with coefficients in $\mathbb{Q}(S)$ for the first step.

Necessary and sufficient condition for constructibility

- When we construct a bigger set $S' \subset S$ with ruler and compasses, we only solve linear and quadratic equations (intersections of lines and/or circles) with coefficients in $\mathbb{Q}(S)$ for the first step.
- In general, our construction consists of producing a "tower of quadratic extensions"

$$\mathbb{Q}(S) = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \ldots \subset \mathbb{F}_k = \mathbb{Q}(S')$$

where each field $\mathbb{F}_{j+1} = \mathbb{F}_j[\alpha_j]$ is obtained by adjoining a point α_j satisfying at most a quadratic equation.

Necessary and sufficient condition for constructibility

- When we construct a bigger set $S' \subset S$ with ruler and compasses, we only solve linear and quadratic equations (intersections of lines and/or circles) with coefficients in $\mathbb{Q}(S)$ for the first step.
- In general, our construction consists of producing a "tower of quadratic extensions"

$$\mathbb{Q}(S) = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \ldots \subset \mathbb{F}_k = \mathbb{Q}(S')$$

  where each field $\mathbb{F}_{j+1} = \mathbb{F}_j[\alpha_j]$ is obtained by adjoining a point α_j satisfying at most a quadratic equation.
- Remark. The "quadratic tower" condition is necessary and sufficient: any such tower starting with $\mathbb{Q}(S)$ consists of points which are constructible step by step from S.

The degree must be a power of 2

- Consequence: $[\mathbb{Q}(S') : \mathbb{Q}(S)]$ must be a power of 2 !

The degree must be a power of 2

- Consequence: $[\mathbb{Q}(S') : \mathbb{Q}(S)]$ must be a power of 2 !
- Theorem (Gauss, just before 1800) A regular n-agon (polygon with n-sides), is constructible if and only if the prime factorization of n is of the form $n = 2^k p_1 \ldots p_m$ where the p_j are Fermat primes, i.e. prime numbers of the form $p_j = 2^{2^{q_j}} + 1$.

The degree must be a power of 2

- Consequence: $[\mathbb{Q}(S') : \mathbb{Q}(S)]$ must be a power of 2 !
- Theorem (Gauss, just before 1800) A regular n-agon (polygon with n-sides), is constructible if and only if the prime factorization of n is of the form $n = 2^k p_1 \ldots p_m$ where the p_j are Fermat primes, i.e. prime numbers of the form $p_j = 2^{2^{q_j}} + 1$.
- Proof. – We are using n-th rooths of 1, i.e. the field $\mathbb{Q}[\omega]$, $\omega^{n-1} + \ldots + \omega + 1 = 0$, of degree $d \leq n - 1$.
  – Degree can be $d < n - 1$ (example $d = 2$ for $n = 6$).
  – Reduction to the case $n = p^r$ is a prime power
  – When $n = p^r$, ω is of degree $d = (p - 1)p^r$ exactly (this has to be proved!). Thus either $p = 2$ or $r = 1$ and $p - 1$ has to be a pover of 2, i.e. $p = 2^s + 1$, and then s itself has to be a power of 2.

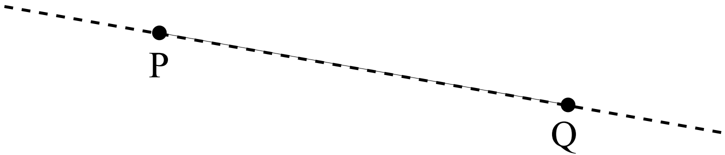
Axioms of construction by origamis (1)

One constructs lines by folding paper; points can be constructed by taking intersections of folding lines.

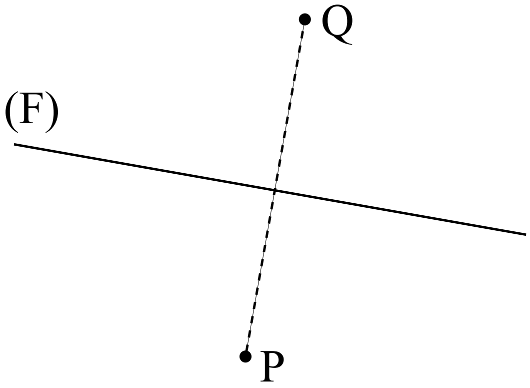
Axioms of construction by origamis (1)

One constructs lines by folding paper; points can be constructed by taking intersections of folding lines.

- Axiom O1. Given two points P ,Q, one can fold paper through line (PQ)

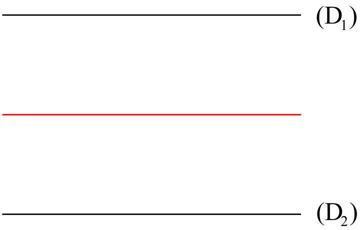


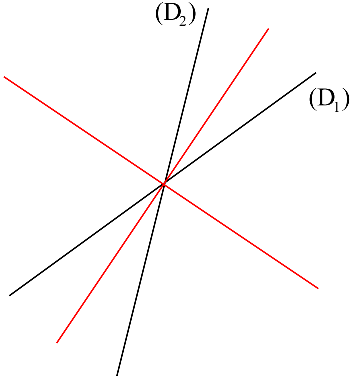
Axiom O2. Given two points P, Q, one can fold paper to bring P to Q (through the median line of segment $[P, Q]$.



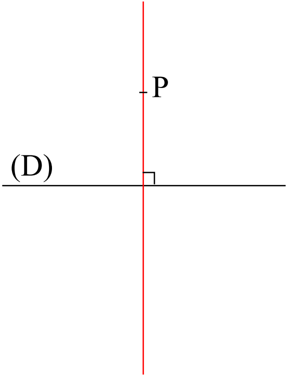
Axioms of construction by origamis (3)

Axiom O3. Given two lines (D_1), (D_2) one can fold paper to bring (D_1) onto (D_2) (through one of the bissecting lines)

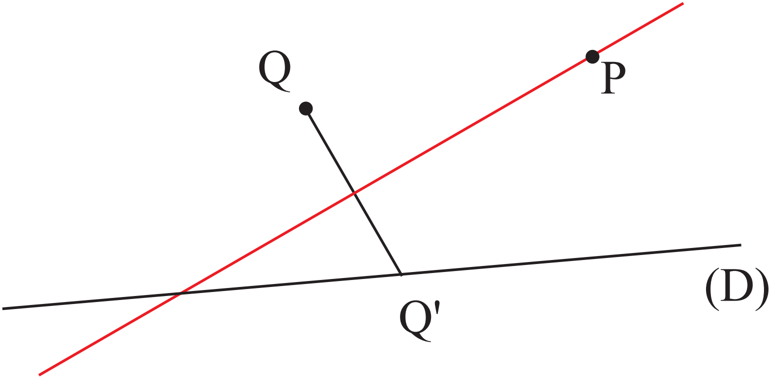




Axiom O4. Given one point P and a line (D), one can fold through point P in such a way that (D) is brought to itself (thus perpendicular to (D) through P)

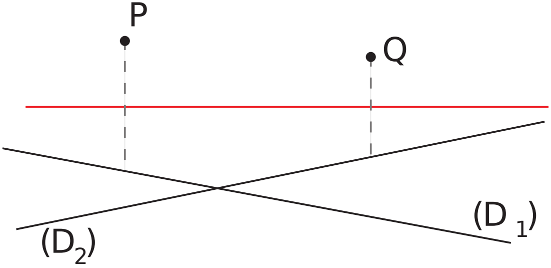


Axiom O5. Given a line (D) and two points P, Q, one can (whenever possible) fold paper through P in such a way that Q is brought to a point of (D).



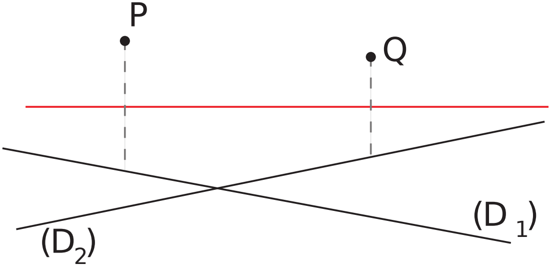
Axioms of construction by origamis (6)

Axiom O6. Given two lines (D_1) and (D_2) and two points P, Q, one can (whenever possible) fold paper to bring P to a point of (D_1) and Q to a point of (D_2)



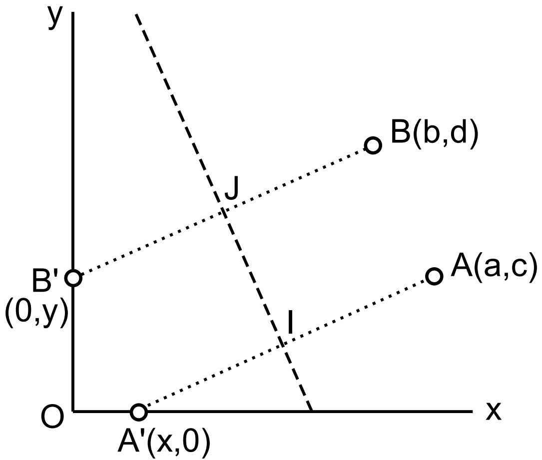
Axioms of construction by origamis (6)

Axiom O6. Given two lines (D_1) and (D_2) and two points P, Q, one can (whenever possible) fold paper to bring P to a point of (D_1) and Q to a point of (D_2)



In fact, axiom O6 can be seen to imply all others. As in the case of compass and ruler, one can see that the axioms allow to take arbitrary integer multiples or quotients, as well as addition, multiplication or division of complex numbers.

Origamis and cubic equations



Problem. Bring $A(a,c)$ given onto $A' \in Ox$ and $B(b,d)$ given onto $B' \in Oy$ by folding.

Origamis and cubic equations (calculation)

One gets $t = \mathrm{slope}(AA') = \mathrm{slope}(BB') \Rightarrow t = \dfrac{d-y}{b} = \dfrac{c}{a-x}$

$I\Big(\dfrac{a+x}{2},\dfrac{c}{2}\Big)$ $J\Big(\dfrac{b}{2},\dfrac{d+y}{2}\Big)$, slope $(IJ) = \dfrac{-1}{t} = \dfrac{d+y-c}{b-(a+x)}$
Therefore

$$x = a - \frac{c}{t}, \quad y = d - bt, \quad \frac{-1}{t} = \frac{2d-c-bt}{b-2a+\frac{c}{t}}$$

whence the equation

$$bt^3 + (c-2d)t^2 + (2a-b)t - c = 0$$

which is equivalent to the most general cubic equation $t^3 + pt^2 + qt + r = 0$ by putting

$$a = \frac{q+1}{2}, \quad b = 1, \quad c = -r, \quad d = -\frac{p+r}{2}.$$

Necessary and sufficient condition for constructibility by origamis

- Theorem: a set S' can be constructed by origamis from $S = \{0, 1, s_3, \ldots, s_n\}$ if and only if there is a tower of field extensions

$$\mathbb{Q}(S) = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \ldots \subset \mathbb{F}_k = \mathbb{Q}(S')$$

where each extension $\mathbb{F}_{j+1} = \mathbb{F}_j[\alpha_j]$ is a quadratic or cubic extension.

Necessary and sufficient condition for constructibility by origamis

- Theorem: a set S' can be constructed by origamis from $S = \{0, 1, s_3, \ldots, s_n\}$ if and only if there is a tower of field extensions

  $$\mathbb{Q}(S) = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \ldots \subset \mathbb{F}_k = \mathbb{Q}(S')$$

  where each extension $\mathbb{F}_{j+1} = \mathbb{F}_j[\alpha_j]$ is a quadratic or cubic extension.

- Corollary. A polygon with n sides can be constructed with origamis if and only if $n = 2^k 3^\ell p_1 \ldots p_m$ where each p_j is a prime number with the property that each $p_j - 1 = 2^{a_j} 3^{b_j}$.

References

James King, Origami constructible numbers, 2004 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.123.6667&rep=rep1&type=pdf

Michael Filaseta Lecture Notes, Section 6, the transcendence of e and π, http://www.math.sc.edu/~filaseta/gradcourses/Math785/Math785Notes6.pdf

Serge Lang, Algebra, Graduate Texts in Mathematics 211, Springer, 3rd edition, 2002.