Straightedge and compass construction: Gauß-Wantzel theorem

Using an idealized ruler (infinite length and only one edge, with no markings on it) and a compass (no minimum or maximum radius, collapses when lifted from the page), what regular polygons can we construct?

Theorem (Gauß Wantzel)

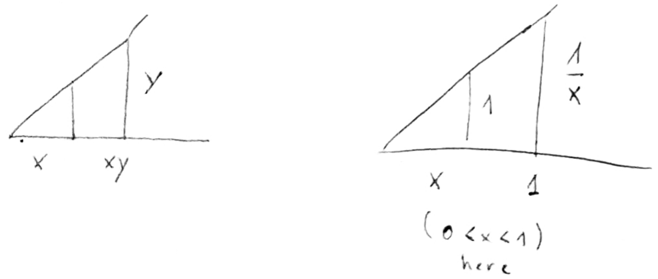
Let $n \geq 2$. The regular n gon is constructible iif $n = 2^k p_1 \cdots p_m$, $k \in \mathbb{N}$, $m \in \mathbb{N}$, p_i's are Fermat primes that are distinct.

I] Constructible Numbers

$\{0, 1\}$ are given. We work in $\mathbb{C}$. A point P is <u>constructible</u> if $\exists P_0, \dots, P_N = P$ with $P_0 \in \{0,1\}$ and for $n < N$, P_{n+1} is an intersection point of two lines/circles using points with indice $< n$.

Using the compass we can construct $\mathbb{Z}$.

Using Thalès:



Obviously constructible points are stable by sum. Which lead to the following definitions:

Def (Field) $(\mathbb{K}, +, \times)$ is a field if: ① verso

$(\mathbb{K}, +)$ is an abelian group

- $\forall x, y \in \mathbb{K}, \quad x + y \in \mathbb{K}$
- $\forall x, y, z \in \mathbb{K}, \quad (x+y)+z = x+(y+z)$
- $\exists\, 0 \in \mathbb{K}, \quad x + 0 = 0 + x = x$
- $\forall x \in \mathbb{K}, \ \exists\, (-x) \in \mathbb{K}, \quad x + (-x) = (-x) + x = 0$
- $x + y = y + x$

$(\mathbb{K}, +, \times)$ is a ring

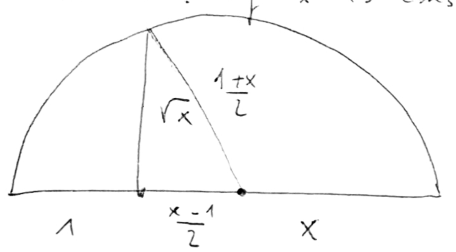
- $\forall x, y \in \mathbb{K}, \quad x \times y \in \mathbb{K}$
- $(x \times y) \times z = x \times (y \times z)$
- $x \times (y+z) = x \times y + x \times z$
- $\exists\, 1 \in \mathbb{K}, \quad x \times 1 = 1 \times x = x$

$(\mathbb{K}, +, \times)$ is a field: $(\mathbb{K}, +, \times)$ is a ring s.t. $\forall x \in \mathbb{K} \setminus \{0\}$, $\exists\, y \in \mathbb{K}$ st

$x \times y = y \times x = 1 \quad (y =: x^{-1})$

Constructible numbers form a field, containing $\mathbb{Q}$. We call this field $\mathcal{C}$.

Even better: if x is constructible, $\sqrt{x}$ is constructible



$(x > 1)$

$0 < x < 1 : \quad \sqrt{x} = \dfrac{1}{\sqrt{\frac{1}{x}}}$

For example $\sqrt{2}$ is constructible and thus, since $\mathcal{C}$ is a ring it contains $\mathbb{Q}[\sqrt{2}] := \{ P(\sqrt{2}),\ P \in \mathbb{Q}[X] \}$ smallest ring containing $\mathbb{Q}$ and $\sqrt{2}$.

$$= \{ a_0 + a_1\sqrt{2} + a_2\sqrt{2}^2 + \dots + a_n\sqrt{2}^n,\ n \geq 0,\ a_i \in \mathbb{Q} \}$$

$$= \{ a_0 + a_1\sqrt{2} \mid a_0, a_1 \in \mathbb{Q} \}$$

$\mathcal{C}$ is a field: it contains $\mathbb{Q}(\sqrt{2}) := \{ \frac{P}{Q}(\sqrt{2}),\ P \in \mathbb{Q}[X],\ Q \in \mathbb{Q}[X] \setminus \{0\} \}$ (smallest field containing $\mathbb{Q}$ and $\sqrt{2}$)

But since: $\dfrac{1}{a + \sqrt{2}b} = \dfrac{a - \sqrt{2}b}{a^2 - 2b^2}$: $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$

$\dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}]) = 2$ notice that $\sqrt{2}$ is a root of $X^2 - 2 \in \mathbb{Q}[X]$.

it is the polynomial with least degree st $\sqrt{2}$ is one root and it belongs to $\mathbb{Q}[X]$.

We use the notation $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) =: [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 = \deg(X^2 - 2)$

Intersection of two lines: the new point is in $\mathbb{K}$ with points in $\mathbb{K}$ (2)

Intersection of line-circle: $\mathbb{K}$ or $\mathbb{K}(\sqrt{x})$

Intersection of circle-circle: $\mathbb{K}$ or $\mathbb{K}(\sqrt{x})$

Hence:

Wantzel Theorem

$z \in \mathbb{C}$ is constructible $\Leftrightarrow$ $\exists\, L_0 = \mathbb{Q} \subset L_1 \subset \dots \subset L_n$ a sequence of fields st $[L_{i+1} : L_i] \leq 2$ and $z \in L_n$.

The $(\Leftarrow)$ is due to the fact that if $[L_{i+1} : L_i] = 2$ and $b \in L_{i+1} \setminus L_i$, $(1, b, b^2)$ is L_i-linearly dependent: $a_0 + a_1 b + a_2 b^2 = 0$ $(a_0, a_1, a_2) \in L_i^3 \setminus \{(0,0,0)\}$

Solving this equation: $b = \dfrac{-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}}{2a_0} \in L_i\left(\sqrt{a_1^2 - 4a_0a_2}\right) \Rightarrow b$ is constructible

ex: We can construct

$$\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5}-1}{4} \quad \text{and} \quad \cos\left(\frac{2\pi}{17}\right) = \frac{1}{16}\left[-1+\sqrt{17}+\sqrt{34-2\sqrt{17}} + \sqrt{68+12\sqrt{17}-4\sqrt{34-2\sqrt{17}}-8\sqrt{34+2\sqrt{17}}}\right.$$

Back to the dimension:

$[\mathbb{C} : \mathbb{R}] = 2$ $(z \in \mathbb{C} : z = a.1 + b.i)$ $2 = \deg(X^2+1)$

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2, a_0, a_1, a_2 \in \mathbb{Q}\}$

$3 = \deg(X^3 - 2)$

$[\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4$

$\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$. $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}][\mathbb{M} : \mathbb{K}]$

$\rightarrow$ a constructible z belongs to a field $\mathbb{K}$ st $[\mathbb{K} : \mathbb{Q}] = 2^m$ for some m.

Gauß - Wantzel

The regular n-gon is constructible iif $n = 2^k p_1 \dots p_m$ p_i's distinct Fermat prime.

First: if we can construct $\widehat{\frac{2\pi}{p}}$ and $\widehat{\frac{2\pi}{q}}$ $p \wedge q = 1$:

Bézout: $pu + qv = 1 \Rightarrow \widehat{\frac{2\pi}{q}} u + \widehat{\frac{2\pi}{p}} v = \widehat{\frac{2\pi}{pq}}$

We just need to prove the result for n prime at some powers: $n = p^\alpha$.

We wish to construct $\omega = e^{\frac{2i\pi}{p^\alpha}}$

It can be constructed iif $\exists L_0 = \mathbb{Q} \subset L_1 \dots \subset L_n = \mathbb{Q}(\omega)$ with $[L_{i+1} : L_i] \leq 2$

If we can construct it then: $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^k$ for some k.

How do we compute $[\mathbb{Q}(\omega) : \mathbb{Q}]$?

↳ Find the polynomial P of least degree in $\mathbb{Q}[X]$ st $P(\omega) = 0$

Any polynomial Q st $Q(\omega) = 0$, $Q \in \mathbb{Q}[X]$ is a multiple of P.

$Q = PA + B \Rightarrow B(\omega) = 0$; $\deg(B) < \deg(P) \Rightarrow B = 0$

P has to be irreducible (can't be written as $P = AB$)

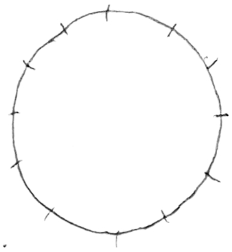
ex: $j = e^{\frac{2i\pi}{3}}$

The minimal polynomial of j in $\mathbb{Q}[X]$ divides $X^3 - 1 = (X-1)(X^2+X+1)$
$= (X-1)(X-j)(X-\bar{j})$

$\Rightarrow P = X^2 + X + 1$

$\omega = e^{\frac{2i\pi}{n}}$ Root of unity

$\Phi_n := \prod_{k \wedge n = 1} (X - \omega^k)$



keep those of order n exactly.

$\deg \Phi_n = \varphi(n) := |\{0 \leq k < n, \ k \wedge n = 1\}|$

$\varphi(p^\alpha) = p^\alpha - p^{\alpha - 1} = p^{\alpha-1}(p-1)$

$\Phi_n \in \mathbb{Z}[X]$ $\left(\Phi_n(X) \mid X^n - 1 \ : \ X^n - 1 = \prod_{d \mid n} \Phi_d(X) \right)$

Φ_n is irreducible

$\Phi_n(\omega) = 0$

$\Rightarrow [\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(p^\alpha) = p^{\alpha-1}(p-1) = 2^k$

(Irreducible: let P the minimal polynomial of ω, ζ st $P(\zeta) = 0$ then for $p \nmid n$ prime, $P(\zeta^p) = 0$)

$p = 2$ or $p > 2$, $\alpha = 1$, $p - 1 = 2^k$

$k = \lambda 2^\beta$ $\quad p = 1 + (2^{2^\beta})^\lambda$ can be divided by $1 + 2^{2^\beta}$ if $\lambda \neq 1$

$(1 + X \mid 1 + X^\lambda$ when λ is odd$)$

$\Rightarrow$ p is a prime Fermat number. $(3, 5, 17, 257, 65537)$

$(\Leftarrow)$ $p = 2^k$ use the bisectors

$p = 2^{k} + 1$ prime Fermat

$\omega = e^{\frac{2i\pi}{p}}$ $\varphi(p) = 2^{2^h} = [\mathbb{Q}(\omega) : \mathbb{Q}]$

Let $G = Gal(\mathbb{Q}(\omega)/\mathbb{Q}) := Aut(\mathbb{Q}(\omega) \to \mathbb{Q}(\omega))$ leaving $\mathbb{Q}$ invariant

$\phi \in G$ ϕ is completely given by $\phi(\omega)$ since

$\phi(P(\omega)) = P(\phi(\omega))$

$\phi(\omega) = \omega^k$ for some k

$$\begin{aligned} G &\longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \\ \sigma_k &\longmapsto k \end{aligned} \qquad \sigma_k(\omega) = \omega^k$$

isomorphism.

$(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic : let σ st $\langle\sigma\rangle = G$.

Then define $L_j = \{ z \in \mathbb{Q}(\omega) : \sigma^{2^j}(z) = z \}$
$= Ker(\sigma^{2^i} - Id)$

$L_0 = \mathbb{Q} \subset L_1 \subset \dots \subset L_k = \mathbb{Q}(\omega)$

$$z = \sum_{h=0}^{2^{h-i-1}-1} g^{2^{i+1}h}(\omega) \in L_{i+1} \setminus L_i$$

$[L_{i+1} : L_i] \geq 2$

$$2^k \leq \prod_{i=0}^{k-1} \underbrace{[L_{i+1} : L_i]}_{\geq 2} = [\mathbb{Q}(\omega) : \mathbb{Q}] = 2^k$$

$\Rightarrow [L_{i+1} : L_i] = 2$

Fundamental theorem of Galois Theory

$\mathbb{K} \subset N$ normal extension $[N : \mathbb{K}] < \infty$

$$\mathcal{E} := \{ \mathbb{L} , \ \mathbb{K} \subset \mathbb{L} \subset N \}$$

$$\mathcal{G} = \{ H < Gal(N/\mathbb{K}) \}$$

$$\begin{aligned} I : \mathcal{G} &\longrightarrow \mathcal{E} \\ H &\longmapsto I(H) := \{ x \in N , \ \sigma(x) = x \ \ \forall \sigma \in H \} \end{aligned}$$

$$\begin{aligned} G : \mathcal{E} &\longrightarrow \mathcal{G} \\ \mathbb{L} &\longmapsto Gal(N/\mathbb{L}) \end{aligned}$$

bijections

Example $n = 15$

$\omega = e^{\frac{2i\pi}{15}}$ $\quad \sigma_k : \omega \mapsto \omega^k \quad k = 1, 2, 4, 7, 8, 11, 13, 14$

$G = Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ has $\varphi(15) = \varphi(3)\varphi(5) = 8$ elements

$$G \simeq (\mathbb{Z}/15\mathbb{Z})^* \simeq (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$$
$$\simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$$

$\eta = e^{\frac{2i\pi}{3}}$

	order	
$\{id\}$	(1)	$\mathbb{Q}[\omega]$
$\langle\sigma_4\rangle$ $\langle\sigma_{11}\rangle$ $\langle\sigma_{14}\rangle$	(2)	$\mathbb{Q}[j, \sqrt{5}]$ $\mathbb{Q}[\eta]$ $\mathbb{Q}[\cos(\frac{2\pi}{15})]$
$\langle\sigma_2\rangle$ $\langle\sigma_7\rangle$ $\langle\sigma_4, \sigma_{11}, \sigma_{14}\rangle$	(4)	$\mathbb{Q}[i\sqrt{15}]$ $\mathbb{Q}[j]$ $\mathbb{Q}[\sqrt{5}]$
G	(8)	$\mathbb{Q}$

④ verso

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{5}] \subset \mathbb{Q}\left[\cos\left(\frac{2\pi}{15}\right)\right]$$

$$\rightsquigarrow \cos\left(\frac{2\pi}{15}\right) = \frac{1+\sqrt{5}+\sqrt{30-6\sqrt{5}}}{8}$$