§ 1. Introduction / motivation

<u>Problem</u> Can we double the cube ?

$\iff$ Can we construct a segment of length $\sqrt[3]{2}$ using a compass and a ruler ?

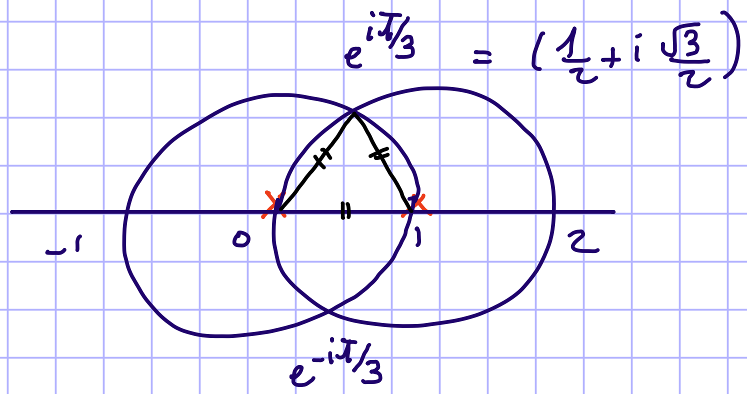
Many compass and ruler constructions that appear simple are first glance went unsolved until the creation of modern algebra.

Abstract algebra provides advanced tools for defining restrictions on which compass and straightedge are possible, and this enabled them to prove once for all that the constructions they had straggled with were in fact, impossible !

<u>Setting</u>:

We imagine this taking place in $\mathbb{R}^2$ where the unit line segment is the segment connecting $(0,0)$ and $(1,0)$.

- Given these two points, we can:
- Use the straightedge to draw horizontal axis ($\mathbb{R}$)
- Use the compass to draw a circle centered in $(0,0)$ and passing through $(1,0)$



We've constructed $(-1,0)$, $(2,0)$; $e^{i\pi/3}$; $e^{-i\pi/3}$ from $(0,0)$ and $(1,0)$.

Now, we have six points and we can continue the process, drawing all possible lines and circles from these points.

For example, we can construct $(1/2, 0)$ by drawing the line connecting $e^{i\pi/3}$ and $e^{-i\pi/3}$.

$$e^{i\pi/3} = \left(\sqrt{3}/2, \tfrac{1}{2}\right)$$

Rule: Given the unit length segment, can we construct a segment of length $\alpha \in \mathbb{R}^+$?
These two problems of constructing points in $\mathbb{R}^2$ and lengths in $\mathbb{R}^+$ are evidently equivalent, and we identify them during this talk.

Goal of the talk: To prove that given the unit segment length, constructible numbers are exactly the one you get from $\{0,1\}$ using the operations $+ , \times , - , \%$ and $\sqrt{\ }$.

§ 2. Formalizing Constructibility

Definition

Given a set $S \subseteq \mathbb{C}$, we say that $z \in \mathbb{C}$ is constructible in one step from S iff there exist points x, y, u, v in S such that

(1) $z \in \overline{xy} \cap \overline{uv}$, or

(2) $z \in \overline{xy} \cap C_u(v)$

(3) $z \in C_x(y) \cap C_u(v)$

Definition: We say that $z \in \mathbb{C}$ is constructible iff there is a finite sequence of points $\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \alpha_n$ with $\alpha_n = z$ st:

α_1 is constructible in one step from $\{0,1\}$

α_2 is constructible in one step from $\{0,1,\alpha_1\}$

$\vdots$

$\alpha_n = z$ is constructible in one step from $\{0,1,\alpha_1,\dots,\alpha_{n-1}\}$

Rmk:

We constructed $1/2$ at the second step of our iteration:
- $e^{i\pi/3}$ and $e^{-i\pi/3}$ from $\{0,1\}$ (2 circles)
- $1/2$ from $\{e^{i\pi/3}, e^{-i\pi/3}\}$ (2 lines)

whereas according to the above definition, it would take 3 steps to do:

- $e^{i\pi/3}$ from $\{0,1\}$
- $e^{-i\pi/3}$ from $\{\underset{\sim}{0}, \underset{\sim}{1}, e^{i\pi/3}\}$
- $1/2$ from $\{0, 1, \underset{\sim}{e^{i\pi/3}}, \underset{\sim}{e^{-i\pi/3}}\}$

<u>Definition</u> Let $S_0 = \{0,1\}$

$S_1 = \{ z \text{ constructible from } S_0 \text{ in one step}\}$

$S_k = \{ z \text{ constructible from } S_{k-1} \text{ in one step}\}$

$(S_1 \subset S_2 \subset \dots S_k)$

is the set of points constructible in at most k steps.

We say that $z \in \mathbb{C}$ is constructible if $z \in S_k$ for some $k \in \mathbb{N}$.

<u>Rmk</u>: It doesn't matter which definition we follow as we are only interested in whether the number of steps to construct an element is finite, not the minimum number of steps it would take. Here I will use the latter.

Having formalized the definition of constructibility we now connect constructible numbers to field theory.

§ 3. Field extension

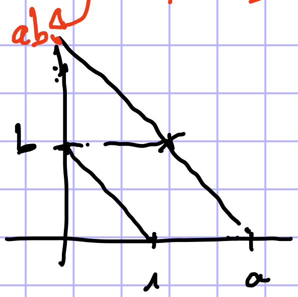
$\mathbb{R}^2 \subset \mathbb{C}$ $\qquad (a,b) \longmapsto a+ib$

$z \in \mathbb{C}$ constructible $\underline{\text{def}}$: its coordinates are constructible.

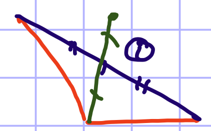
<u>Proposition</u>: If $x, y \in \mathbb{C}$ are constructible, so are $x \pm y$, xy, x/y $(y \neq 0)$.

<u>Proof</u>

easy eg. Thalès



to construct the parallel:



① mid pt of the diag

② 2nd diag

↳ get a parallelogram

<u>Corollaries</u>:

- The set of constructible numbers is a subfield of $\mathbb{C}$
- $\mathbb{Q}$ is constructible.
- Note that the set of all constructible numbers is a field intermediate between $\mathbb{Q}$ and $\mathbb{C}$.
- To study constructible numbers one needs to study how fields are enlarged to contain certain elements.

• Given two fields F and K st $F \subseteq K$, we say that F is a subfield of K. We desribe the reverse relationship as "a field extension."

<u>Definition</u> (field extension)

Let F and K be fields.

We say that K is a field extension of F if F is a subfield of K. We write K/F.
↳ "K over F"

<u>Examples</u> $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$

• Given a field extension K/F (think of $\mathbb{R}/\mathbb{Q}$) and $\alpha \in K$, we want to know what is the field "generated" by appending α to F and "closing" the set under the operations in the field.

eg. appending $\sqrt{2}$ to $\mathbb{Q}$.

<u>Definition</u> Let K/F and $\alpha_1, \dots, \alpha_n \in K$.

$F(\alpha_1, \dots, \alpha_n)$ is the minimal (smallest) subfield of K containing F and all α_i, $1 \leq i \leq n$.

<u>Examples:</u>

1) If F is a field and $\alpha \in F$, $F(\alpha) = F$.

2) $\mathbb{R}(i) = \{a + ib \mid a, b \in \mathbb{R}\} \subseteq \mathbb{C}$

3) $\mathbb{Q}(\sqrt{2}) = \{a + \sqrt{2}b, \quad a, b \in \mathbb{Q}\}$

<u>Fact:</u>

Given a field extension F/K, F is a vector space over K.

<u>Examples:</u>

- $\mathbb{C}$ is an $\mathbb{R}$-vector space of dimension 2. (base $(1, i)$)
- $\mathbb{Q}(\sqrt{2})$ is a $\mathbb{Q}$-vector space of dimension 2. (base $(1, \sqrt{2})$)
- $\mathbb{R}$ is a $\mathbb{Q}$ vector space of ∞ dimension.

the dimension of these vector spaces gives a "size" of the field extension

<u>Definition</u> K/F a field extension

The degree of K/F is the dimension of K as an F vector space.

We write $[F : K] = n$

Eg. $[\mathbb{C} : \mathbb{R}] = 2$ $\rightsquigarrow$ deg $x^2 + 1$ $\qquad [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2 \rightsquigarrow \deg x^2 - 2$

poly with $\sqrt{2}$ as a root

minimal degree among such poly

Theorem 1: K/F, $\alpha \in K$.
Suppose there exists a polynomial with coef in $F[X]$ with root α. Among the polynomials of which α is a root, there exist one f_α which monic and of minimal degree called minimal polynomial of α. Furthermore

$$[F(\alpha):F] = \deg f_\alpha$$

(if irreducible + monic $\Rightarrow$ minimal)

Theorem 2: Let L/K and K/F
Then L/F is a field extension.
In addition, the degrees $[L:K]$ and $[K:F]$ are finite iff $[L:F]$ is finite and in this case:

$$[L:F] = [L:K][K:F]$$

§4. Main theorem

If α is constructible, then $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2^k$ for some $k \in \mathbb{N}$.

Proof

(A) α is constructible $\Rightarrow$ $\exists k \in \mathbb{N}$ st $\alpha \in S_k$

$$\begin{array}{c} \mathbb{Q}(S_k) \\ | \\ \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q} \end{array}$$

$\Rightarrow$ $[\mathbb{Q}(\alpha):\mathbb{Q}] \mid [\mathbb{Q}(S_k):\mathbb{Q}]$

hence it is enough to prove that $[\mathbb{Q}(S_k):\mathbb{Q}]$ is a power of 2.

(B) $\mathbb{Q}(S_0) = \mathbb{Q} - \mathbb{Q}(S_1) - \cdots - \mathbb{Q}(S_{k-1}) - \mathbb{Q}(S_k)$

By induction in k, to prove that $[\mathbb{Q}(S_k):\mathbb{Q}]$ is a power of 2, it is enough to prove that $[\mathbb{Q}(S_k):\mathbb{Q}(S_{k-1})]$ is a power of 2.

(C) $\mathbb{Q}(S_{k-1}) - \mathbb{Q}(S_{k-1}, \alpha_1) - \mathbb{Q}(S_{k-1}, \alpha_1, \alpha_2) - \cdots - \mathbb{Q}(S_k)$

where $\alpha_i \in S_k$ is constructible in one step from S_{k-1} by definition.

hence to prove the theorem, we are reduced to prove that $[\mathbb{Q}(S,z):\mathbb{Q}(S)]$ is a power of 2 if z is constructible in one step from S. We will prove that this degree ≤ 2

Rule: We can assume that $i \in S$.
($i \in S_k$ $\forall k \geq 1$ because i is constructible in 1 step from S_0.)

z is constructible in one step from S iff it lies in the intersection of two lines, a line and a circle or two circles that are constructible from S.

1) If z is the intersection of 2 lines constructible from $\mathbb{Q}(S)$, then z is the solution to a system of two linear equations with coef in $\mathbb{Q}(S)$.
Hence, if $z = x+iy$, $[\mathbb{Q}(S,x,y):\mathbb{Q}] = 1$

since $z \in \mathbb{Q}(S,x,y)$

$[\mathbb{Q}(S,z):\mathbb{Q}(S)] = 1$

(2) if z is the intersection of a line and a circle constructible from $\mathbb{Q}(S)$, then it is a solution to a system of a linear equation and a quadratic equation, both with coef in $\mathbb{Q}(S)$.

$$\begin{cases} ax + b = y & a, b \in \mathbb{Q}(S) \\ (x-c)^2 + (y-d)^2 = r^2 , & a, b, r \in \mathbb{Q}(S) \\ & c, d \end{cases}$$

$\hookrightarrow$ We get a polynomial of degree 2 with root $x \Rightarrow [\mathbb{Q}(S, x) : \mathbb{Q}(S)] \leq 2$ ($\ni y$)

since $z \in \mathbb{Q}(S, x) = \mathbb{Q}(S, x, y)$

$[\mathbb{Q}(S, z) : \mathbb{Q}(S)] \leq 2$

③ If z is the intersection of two circles constructible from $\mathbb{Q}(S)$, we obtain two quadratic equations of the form $(x-a)^2+(y-b)^2=r^2$, with $a, b, r \in \mathbb{Q}(S)$

$$\begin{cases} (x-a)^2+(y-b)^2=r^2 \\ (x-a')^2+(y-b')^2=r'^2 \end{cases}$$

$$(2x-a-a')(a'-a)+(2y-b+b')(b'-b)=r^2-r'^2$$

linear eq between x and y with coef in $\mathbb{Q}(S)$

... As in the previous case $\Rightarrow [\mathbb{Q}(S,z):\mathbb{Q}(z)] \leq 2$

$\blacksquare$

<u>Comment</u>: the theorem gives a necessary condition for a number to be constructible

But from the proof it appears that a number α is constructible iff $[\mathbb{Q}(\alpha):\mathbb{Q}]$ can be decomposed into a tower of quadratic extensions.

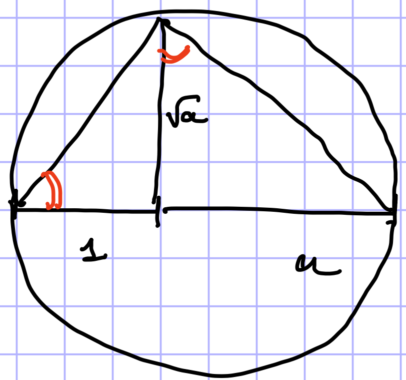
For example, any square of a rational number is constructible as the degree of the corresponding field ext. is 2.

- The proof doesn't provide a way to construct a number geometrically but if one can decompose the field ext. into a tower of quadratic field extensions, we know from which numbers we can construct it.

Eg: Construct $\sqrt{\sqrt{2}}$

$$\begin{tikzcd} \mathbb{Q} \arrow[rr, dash, "4"] \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{\sqrt{2}}) \\ & \mathbb{Q}(\sqrt{2}) \arrow[ur, dash, "2"'] & \end{tikzcd}$$

if we construct geometrically $\sqrt{2}$, we can construct $\sqrt{\sqrt{2}}$ from it.



<u>Counter example?</u> $f(x) = x^4 + 8x + 12$

The Galois group of f is $A_4 \subseteq S_4$

Let α be a root of f.

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^2 = 4$$

Does $\mathbb{Q}(\alpha)$ has a quadratic subfield extension ?
By the Galois main theorem, it is the case iff the Galois group of α has a subgroup of index 2.
But A_4 doesn't !

<u>Discussion</u> :

It seems that for polynomials of degree 4, its roots are non constructible iff its Galois group is A_4.

§ 6. Impossibility proofs

Corollary 1: We cannot double the cube

Proof: We show we cannot double the unit cube. To do so requires to construct $\sqrt[3]{2}$.

The minimal poly of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $X^3 - 2$ (enough to show it is irred)

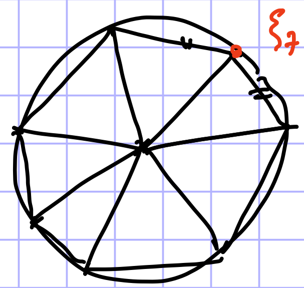
$\Rightarrow \quad [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^j \quad \forall j \in \mathbb{N}$

hence $\sqrt[3]{2}$ is non constructible

Einsenstein crit.
$f \in \mathbb{Z}[x] = x^n + a_{n-1}x^{n-1} + \dots$
$p \mid a_i \ \forall i \leq n-1, \ p^2 \nmid a_n$

Corollary 2: We cannot construct a regular heptagon.

Proof: $\Rightarrow$ construct $e^{2i\pi/7} =: \zeta_7$



$\zeta_7 = e^{2i\pi/7}$

ζ_7 root of $x^7 - 1 = (x-1)(x^6 + x^5 + \dots + 1)$

irreducible $\Rightarrow$ minimal polynomial

$[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6 \neq 2^j \quad \forall j \in \mathbb{N}$

$\blacksquare$

Corollary 4: We cannot square the circle

Proof: The area of the unit circle is π, so to construct a square of area π, we need to construct $\sqrt{\pi}$.

If $\sqrt{\pi}$ is constructible, π is constructible as well.

But $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$

$\rightarrow$ transcendent number.

$\square$

Corollary 4: There is no construction that trisects an arbitrary angle.

Proof: We show that we cannot trisect $60°$, which is constructible.

Constructing $20° \Leftrightarrow$ construct 9-th root of unity $\xi_9 := e^{2i\pi/9}$

$\Rightarrow \xi_9 + \overline{\xi_9}$ is constructible

$$(\xi_9 + \overline{\xi_9})^3 = 1 + 3(\xi_9 + \overline{\xi_9})$$

$\Rightarrow$ is a root of $X^3 - 1 - 3X$

+ irreducible $\rightarrow$ minimal polynomial of ξ_9 over $\mathbb{Q}$

$$[\mathbb{Q}(\xi_9 + \overline{\xi_9}) : \mathbb{Q}] = 3.$$

$\square$