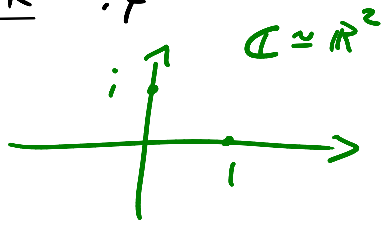
4.7 Constructions with ruler and compass

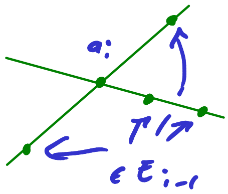
<u>Def:</u> $K \subset \mathbb{C}$

An element $a \in \mathbb{C}$ is <u>constructible over K</u> if there exists a tower

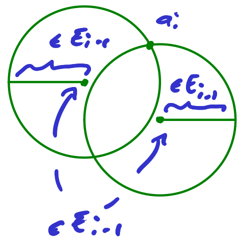


$$K = E_0 \subset E_1 \subset \_\_ \subset E_k$$

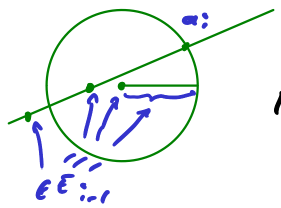
such that $a \in E_k$ and such that $E_i = E_{i-1}(a_i)$ where a_i is the intersection point



- of two lines that contain each 2 distinct points of E_{i-1};



- of two circles with center in E_{i-1} and radius in $E_{i-1} \cap \mathbb{R}$;
- of a line and a circle with the previous properties.



Note that lines are defined by linear equations and circles are defined by quadratic equations. Thus $[E_i : E_{i-1}] = 1$ or 2.

<u>Exercise:</u> This definition coincides with the definition of the first lecture.

<u>Thm 1:</u> $K \subset \mathbb{C}$
$a \in \mathbb{C}$ algebraic over K
$L = K(a)^{\text{norm}}$ normal closure of $K(a)/K$

Then a is constructible over K if and only if $[L:K]$ is a power of 2.

proof: "$\Rightarrow$": Assume that a is constructible over K, i.e. there is a tower

$$K = E_0 \subset \dots \subset E_k$$

of quadratic extensions $E_i = E_{i-1}(a_i)/E_{i-1}$ such that $a \in E_k$. The normal closure E_k^{norm} of E_k/K is generated by

$$\{\sigma(a_i) \mid i = 1 \dots k,\ \sigma : E_k \underset{K}{\to} \mathbb{C}\}$$

Adjoining the elements $\sigma(a_i)$ successively yields a tower

$$K = E_0 \subset \dots \subset E_k \subset E_{k+1} = E_k(\sigma(a_1)) \subset \dots \subset E_\ell = E_k^{norm}$$

of quadratic (or trivial) extensions.

Thus $[E_k^{norm} : K] = 2^n$ for some $n \geq 0$.

Since $K(a) \subset E_k$, $L = K(a)^{norm} \subset E_k^{norm}$

and $[L:K] \mid [E_k^{norm} : K] = 2^n$.

$\Rightarrow [L:K] = 2^m$ for some $m \leq n$. ↯

"$\Leftarrow$": Assume $[L:K] = 2^n$ for some $n \geq 0$.

$\Rightarrow G = Gal(L/K)$ is a 2-group

$\Rightarrow G$ solvable (Lemma 4.2.5)

$\Rightarrow \exists$ composition series

$$\{e\} \lhd G_0 \lhd \dots \lhd G_e = G$$

with factors $\mathbb{Z}/2\mathbb{Z}$.

- Define $E_i = L^{G_i}$. Then

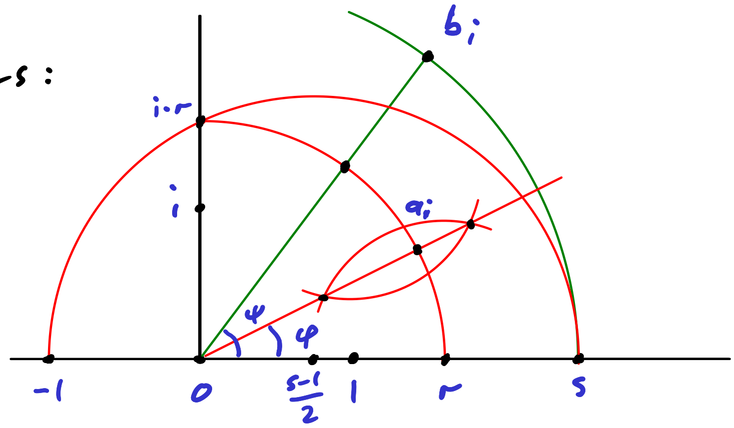
$$K = E_e \subset \text{—} \subset E_0 = L$$

is a tower of quadratic extensions with $\mathrm{Gal}(E_{i-1}/E_i) = \mathbb{Z}/2\mathbb{Z}$.

- Since $\zeta_2 = -1 \in E_i$, E_{i-1}/E_i is Kummer. By Thm. 4.5.1, $E_{i-1} = E_i(a_i)$ for some $a_i \in E_{i-1}$ with $b_i = a_i^2 \in E_i$.

- a_i can be constructed from b_i (and 0 and 1) as follows:

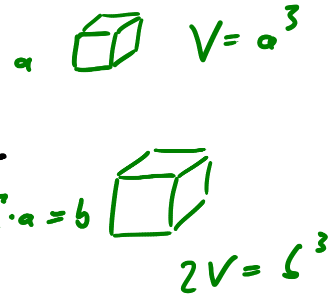
$s = |b_i|$
$\psi = \arg b_i$
$r = |a_i| = \sqrt{s}$
$\varphi = \arg a_i = \frac{1}{2}\psi$



This shows that a_i is constructible over E_i, and thus all elements of E_{i-1} (using the constructions for $+, -, \cdot, :$ from the first lecture).
Thus by an easy induction, a is constructible over K. $\square$

Cor 2: Not every cube can be doubled.

proof: · Given a cube with side length a, then the cube with twice the volume has side length $\sqrt[3]{2}\cdot a$.



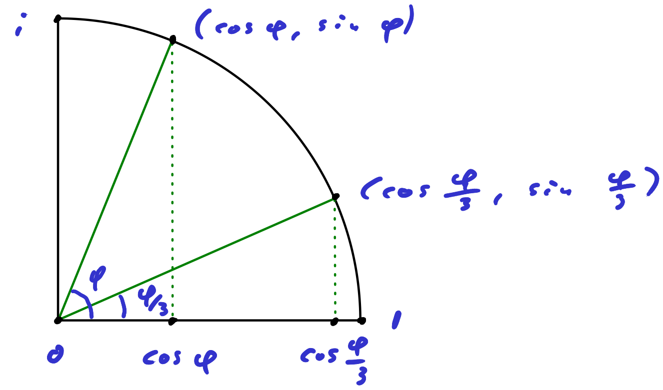
· For example, take $a=1$. Then $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is cubic and $[\mathbb{Q}(\sqrt[3]{2})^{\text{norm}} : \mathbb{Q}] = 6$ is not a power of 2.

· Thus by Thm. 1, $\sqrt[3]{2}$ is not constructible $/\mathbb{Q}$. □

Cor 3: Not every angle can be trisected.

proof: · An angle φ corresponds to $(\cos\varphi, \sin\varphi)$ as a point of the unit circle.

We will show that we cannot construct $\cos\frac{\varphi}{3}$ from $\cos\varphi$ in general.



· Let $\psi = \frac{\varphi}{3}$, i.e. $\varphi = 3\psi$. Since

$$\cos 3\psi = 4\cos^3\psi - 3\cos\psi,$$

$a = \cos\psi$ is a root of $f = 4T^3 - 3T - b$

for $b = \cos 3\varphi$.

- If for instance $b = 3/4$, then

  $4f = 16T^3 - 12T - 3$ is irreducible over $\mathbb{Q}$

  (Eisenstein criterion for $p=3$ + Gauß Lemma).

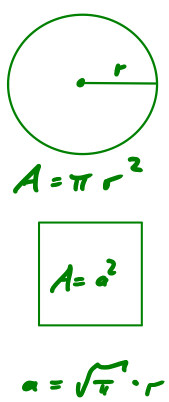
  Thus f is irreducible over $\mathbb{Q}$ and

  $\mathbb{Q}(\alpha)/\mathbb{Q}$ cubic, which shows that

  $[\mathbb{Q}(\alpha)^{\text{norm}} : \mathbb{Q}]$ cannot be a power of 2. $\square$

<u>Cor 4:</u> The circle cannot be squared.

<u>proof:</u> Given a circle with radius r, its area is $A = \pi r^2$. Thus a square with area A must have side length $\sqrt{\pi}\cdot r$. By Lindemann (1882), π is not algebraic over $\mathbb{Q}$, thus $\sqrt{\pi}$ is not algebraic over $\mathbb{Q}$ and therefore not constructible over $\mathbb{Q}(r)$ (for general r) $\square$



<u>Lemma 5:</u> $n = \prod_{i=1}^{r} p_i^{e_i} \in \mathbb{N}$ where $p_1 - p_r$ are distinct prime numbers, $e_1 - e_r \geq 1$

Then $$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1).$$

proof: • By the Chinese remainder theorem,

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod \mathbb{Z}/p_i^{e_i}\mathbb{Z}$$

$$\Rightarrow (\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times.$$

• For each i, we have

$$\#(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times = \#(\mathbb{Z}/p_i^{e_i}\mathbb{Z}) - \#\{\overline{kp}\}_{k\geq 0}$$

$$= p_i^{e_i} - p_i^{e_i-1} = p_i^{e_i-1}(p_i-1). \qquad \square$$

Cor 6: The regular n-gon is constructible over $\mathbb{Q}$ if and only if there is a finite subset $I \subset \mathbb{N}$ and an $r \in \mathbb{N}$ such that

$$n = 2^r \cdot \prod_{i\in I} \left(2^{(2^i)}+1\right)$$

and such that $2^{(2^i)}+1$ is prime for all $i \in I$.

proof: • The regular n-gon is constructible over $\mathbb{Q}$ if and only if ζ_n is constructible over $\mathbb{Q}$. Since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois, this is the if and only if $\varphi(n) = [\mathbb{Q}(\zeta_n):\mathbb{Q}]$ is a power of 2 (by Thm. 1).

- Consider the prime decomposition $n = \prod p_i^{e_i}$.

  Then $\varphi(n) = \prod p_i^{e_i - 1}(p_i - 1)$ by Lemma 5.

  The factor $p_i^{e_i-1}(p_i - 1)$ is a power of 2 if and only if

  (1) $p_i = 2$ and e_i arbitrary, or

  (2) $p_i - 1 = 2^j$ and $e_i = 1$.

- If $j = k \cdot \ell$ for $\ell > 1$ odd, then

  $$2^j + 1 = (2^k + 1)\left(2^{(\ell-1)k} - 2^{(\ell-2)k} + \_ + 2^{2k} - 2^k + 1\right)$$

  is not prime. Thus if 2^j is prime, then $j = 2^i$ for some $i \geq 0$.

- Thus n is constructible iff

  $$n = 2^r \cdot \prod_{i \in I} \left(2^{(2^i)} + 1\right),$$

  and $2^{(2^i)} + 1$ is prime for all $i \in I$. $\square$

<u>Def</u>: The <u>i-th Fermat number</u> is $F_i = 2^{(2^i)} + 1$ for $i \geq 0$.

If F_i is prime, then it is called a <u>Fermat prime</u>.

Fermat number	value	prime ?
F_0	$2^{(2^0)}+1 = 3$	yes
F_1	$2^{(2^1)}+1 = 5$	yes
F_2	$2^{(2^2)}+1 = 17$	yes
F_3	$2^{(2^3)}+1 = 257$	yes
F_4	$2^{(2^4)}+1 = 65.537$	yes
F_5	$2^{(2^5)}+1 = 4.294.967.297$	no (Euler)
$\vdots$		
F_{32}	$\sim 10^9$ digits	no
F_{33}	$\sim 10^{10}$ digits	first unknown
$\vdots$		
$F_{5.523.858}$	$\sim 10^{1.700.000}$ digits	no (largest known)

Conj: F_i is not prime for $i \geq 5$.