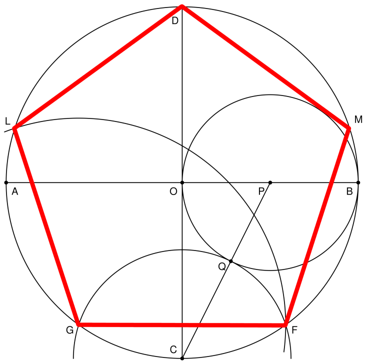
What are...the limits of straightedge and compass?

Or: Field and Galois theory, application 1

The rules of the game



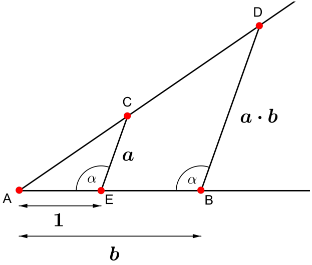
- Start with $\{0, 1\} \subset M \subset \mathbb{R}^2 \cong \mathbb{C}$ Initialization
- We can construct lines containing two points from M Straightedge
- We can construct circles with center and another point from M Compass
- We can increase M successively by points obtained via intersecting constructed lines/circles Game step

How is this algebra?

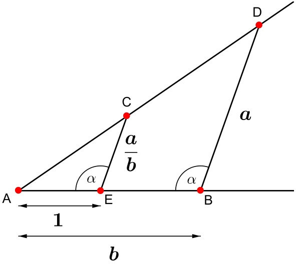
Lemma. $\hat{M}$, containing all points constructible from M, satisfies:

- $i \in \hat{M}$
- $a \in \hat{M}$ implies that $|a|$, $\Re(a)$, $\Im(a)$ and $\bar{a}$ are in $\hat{M}$
- $a, b \in \hat{M}$ implies $a + b \in \hat{M}$ and $-a \in \hat{M}$
- $a, b \in \hat{M}$ implies $a \cdot b \in \hat{M}$ and $a/b \in \hat{M}$ (if $b \neq 0$)

$a \cdot b \rightsquigarrow$



$\frac{a}{b} \rightsquigarrow$

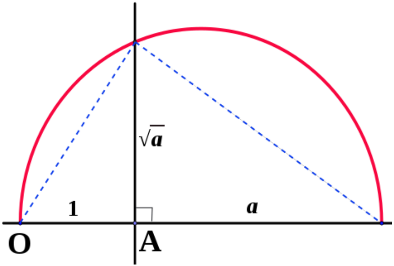


Main observation Constructible points form a subfield of $\mathbb{C}$

Constructible points form a "quadratic subfield" of $\mathbb{C}$

Lemma. $\hat{M}$, containing all points constructible from M, is quadratically closed:

- $a \in \hat{M}$ implies $\sqrt{a} \in \hat{M}$



- Conversely, any constructible point can be obtained by the operations $+, -, \times, \div$ and iterated $\sqrt{\_}$

Thus, for $\mathbb{K} = \mathbb{Q}(M \cup \overline{M})$ we have $[\mathbb{K}(z) : \mathbb{K}] = 2^d$ for some d A power of 2

For completeness: The formal statement

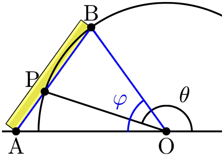
Let $\mathbb{K} = \mathbb{Q}(M \cup \overline{M})$ and $z \in \mathbb{C}$, then the following are equivalent

(a) $z \in \hat{M}$

(b) There are field extensions $\mathbb{K} = \mathbb{K}_0 \subset \ldots \subset \mathbb{K}_n \subset \mathbb{C}$ with $z \in \mathbb{K}_n$ and $[\mathbb{K}_i : \mathbb{K}_{i-1}] = 2$

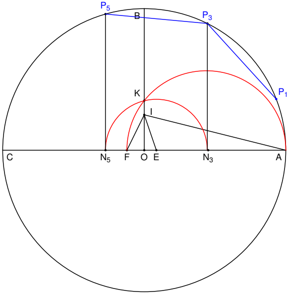
(c) There is a Galois extension $\mathbb{L}$ over $\mathbb{K}$ with $z \in \mathbb{L}$ and $[\mathbb{L} : \mathbb{K}] = 2^d$ for some d

- This shows that trisecting an angle, doubling the cube, squaring the circle *etc.* are impossible with straightedge and compass



- This also gives an effective criterion when the regular n-gon is constructible by straightedge and compass

Constructible polygons



- Gauss—Wantzel The regular n-gon is constructible by straightedge and compass if and only if
$$n = 2^d \cdot p_1 \cdot \ldots \cdot p_k$$
for prime numbers p_j of the form $2^{2^j} + 1$
- The $n = 17$-gon works, as Gauss showed

$$16 \cos \frac{2\pi}{17} = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$$

Thank you for your attention!

I hope that was of some help.