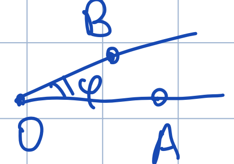
Construction for a heptadecagon

Lecture 6

Df. (points constructible by ruler & compass)
$P_0 = (0,0)$, $P_1 = (1,0)$. Suppose we have constructed $(P_0, \dots, P_n) =: S_n$. Then P_{n+1} is one of the following
1) the intersection of 2 lines, each joining 2 points of S_n
2) — " — circles each with centre a point of S_n and radius the distance between 2 points of S_n
3) — " — circle & line — " —

Similarly $a \in \mathbb{R}$ is constructible if $\exists$ a constructible point on $x^2 = a^2$, an angle is constructible:

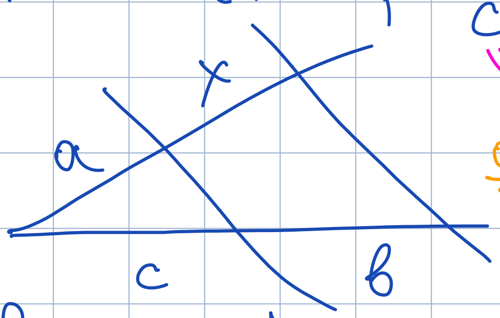


$\Rightarrow \exists$ a constructible C s.t. $\angle COA = \varphi$

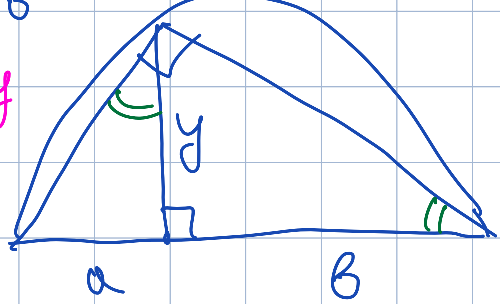
Euclid's Elements contains constructions for the regular triagle, square, pentagon, so $n = 3, 4, 5$ and 15. Also, clearly, having the regular n-gon we can construct the regular $2n$-gon.

L. Let a, b, c be constructible numbers (or a polyquadratic numbers). Then $a \pm b$, $\frac{ab}{c}$, $\sqrt{ab}$ are also constructible.

$\frac{ab}{c} = x$, $\sqrt{ab} = y$



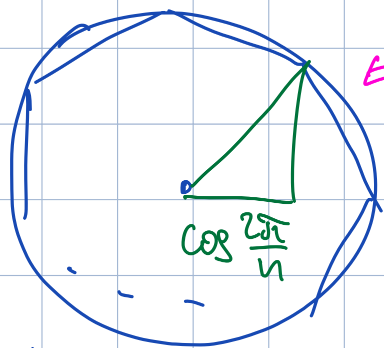
$\frac{a}{x} = \frac{c}{b}$



$\frac{a}{y} = \frac{y}{b}$

So, we have all arithmetic operations & $\sqrt{\cdot}$.

For example, we know that $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$



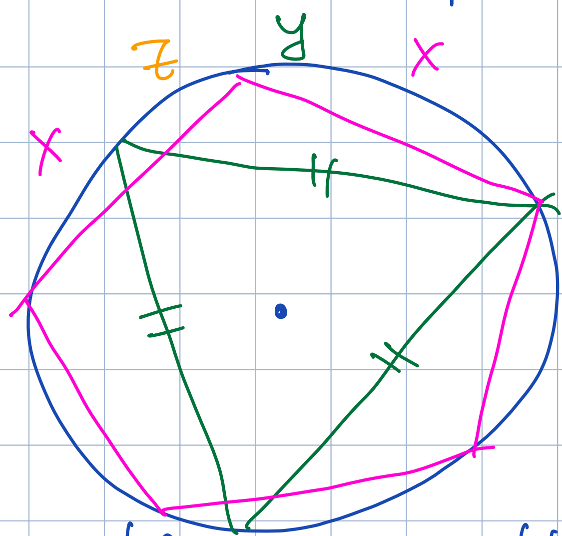
$\Downarrow$

this is a constructible number

$\Downarrow$

we can construct the regular pentagon by ruler & compass.

Let $n=15$:



$x = \frac{2\pi}{5}$

$y = \frac{2\pi}{3}$

$z = \frac{2\pi}{5}\cdot 2 - \frac{2\pi}{3} = \frac{2\pi}{15}$

Similarly, if $\gcd(n,m)=1$, then thanks to the Euclidean algorithm $\exists\, u,v$ s.t. $1 = un + vm \Rightarrow \frac{1}{mn} = \frac{u}{m} + \frac{v}{n}$. Thus, if

n-gon & m-gon are constructible and $\gcd(n,m)=1 \Rightarrow$ the regular nm-gon is also constructible. Therefore, it is enough to construct p^k-gon, $p>2$ is a prime number

Th (Gauss) One has

$$\cos\frac{2\pi}{17} = \frac{\sqrt{17}-1}{16} + \frac{1}{16}\sqrt{34-2\sqrt{17}} + \frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{170+38\sqrt{17}}}$$

In particular, the regular 17-gon is constructible.

We can look at the constructible numbers as a field tower

$$\mathbb{Q} \overset{2}{—} K_1 \overset{2}{—} K_2 \overset{2}{—} \dots \overset{2}{—} K_m$$

$K \overset{2}{—} K(\sqrt{D})$, $D \in K$, $\sqrt{D} \notin K$ and, conversely, if $K \overset{2}{—} L$, then $\forall \alpha \in L \setminus K \Rightarrow 1, \alpha, \alpha^2$ are dependent over $K \Rightarrow \exists\, s, t \in K$ s.t. $\alpha^2 = s\alpha + t$

Thus $\left(\alpha - \frac{s}{2}\right)^2 = t + \frac{s^2}{4}$ and hence

$$L = K(\alpha) = K\left(\sqrt{t + \frac{s^2}{4}}\right).$$

In other direction $\forall$ constructible point is polyquadratic since $\forall$ circle and $\forall$ line is defined by an equation of degree $\leq 2 \Rightarrow$ to find the required intersection we solve some quadratic equations (there is a subtlety here with the selection of random points).

Cor. Let $a \in \mathbb{R}$ is constructible. Then $[\mathbb{Q}(a):\mathbb{Q}] = 2^n$

Cor. The cube cannot be duplicated by any ruler and compass construction.

Cor. It is not possible to trisect any given angle.

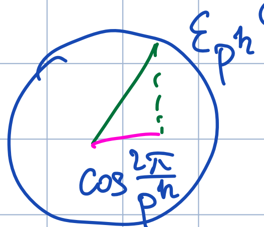
Pf. Take $\alpha = \frac{\pi}{3} \Rightarrow \frac{\alpha}{3} = \frac{\pi}{9}$. Further, $\cos\alpha = \frac{1}{2}$ and hence as in the Vieta method we have

$$\overbrace{4(\cos\alpha)^3 - 3\cos\alpha}^{\cos 3\alpha} - \frac{1}{2} = 0$$

and $f(t) = t^3 - 3t - 1$ is irreducible over $\mathbb{Q} \Rightarrow [\mathbb{Q}(\cos\alpha) : \mathbb{Q}] = 3 \neq 2^n$ and this is a contradiction. ■

In particular, we have proved that it is not possible to construct the regular 9-gon.

To constuct the regular p^k-gon it is more convenuent to have deal with $\mathbb{C}$ (obviously, the whole theory remains true)



$$x^2 - 2\cos\varphi\, x + 1 = 0 \Leftrightarrow x = \cos\varphi \pm i\sin\varphi$$

We know that $\deg \varepsilon_p = p-1$ (since $\overbrace{x^{p-1} + \ldots + 1}^{\Phi_p(x)}$ is irreducible). Hence if p-gon is constructible, then $p = 1 + 2^s$ for a certain s

Exercise $M^{\mathbb{Q}}_{\varepsilon_{p^k}}(x) = \dfrac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = \Phi_p\left(x^{p^{k-1}}\right)$. In particular, $\deg \varepsilon_{p^k} = p^{k-1}(p-1)$.

Therefore, if p^k-gon is constructible, then $k=1$

We have $p = 1+2^s$. If s has an odd divisor, say, d, then $1+2^s \vdots 1+2^{\frac{s}{d}}$ (e.g. $1+2^6 = 1+2^{2\cdot 3} \vdots 1+2^2$)
Thus

$$\boxed{p = 1+2^{2^t}}$$ (Fermat numbers)

Thm (Gauss–Wantzel) The regular n-gon is constructible by ruler and compass iff $n = 2^r p_1 \dots p_s$, where p_j are Fermat primes, $r \in \mathbb{Z}$, $r \geq 0$.

$\Leftarrow$ Gauss, $\Rightarrow$ Wantzel.

Now let $n = 17$. We know that for $\varepsilon = \varepsilon_{17}$ one has $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 16$. We want

$$\mathbb{Q} \overset{2}{—} K_1 \overset{2}{—} K_2 \overset{2}{—} K_3 \overset{2}{—} K_4 = \mathbb{Q}(\varepsilon)$$

Exercise $\exists\, \alpha$, $\deg \alpha = 4$ but $\not\exists\, K$ s.t. $\mathbb{Q} \underset{2}{—} K \underset{2}{—} \mathbb{Q}(\alpha)$

Put $K_3 = \mathbb{Q}\left(\cos \frac{2\pi}{17}\right)$ (then $K_3 \overset{2}{—} K_4$)
We know that $\deg \alpha = \#$ roots of μ_α $= \#$ conjugates of α. The roots of μ_α are

(1) $\varepsilon, \varepsilon^2, \dots, \varepsilon^{16}$ and $\forall\, \alpha \in \mathbb{Q}(\varepsilon)$ has the form

$\in \mathbb{Q}[\varepsilon]$

$\alpha = \alpha(\varepsilon) = a_0 + a_1 \varepsilon + \dots + a_{15}\varepsilon^{15}$, where $a_j \in \mathbb{Q}$ (2)

If we replace ε to ε^j, then we obtain all algebraic conjugates of α. Thus it is more convenient to use basis (1). Gauss' idea is to use geometric progression but not arithmetic. Namely, we know that $\mathbb{Z}_{17}^*$ is a cyclic group, e.g. $\mathbb{Z}_{17}\setminus\{0\} = \{1, 3, 3^2, \dots, 3^{15}\}$. Thus, we can write

$\forall\ \alpha_0 = a_0\varepsilon + a_1\varepsilon^3 + a_2\varepsilon^{3^2} + \dots + a_{15}\varepsilon^{3^{15}}$. Then

$$\alpha_1 = a_0\varepsilon^3 + a_1\varepsilon^{3^2} + a_2\varepsilon^{3^3} + \dots + a_{15}\varepsilon$$
$$\alpha_2 = a_0\varepsilon^{3^2} + a_1\varepsilon^{3^3} + a_3\varepsilon^{3^4} + \dots + a_{15}\varepsilon^3$$

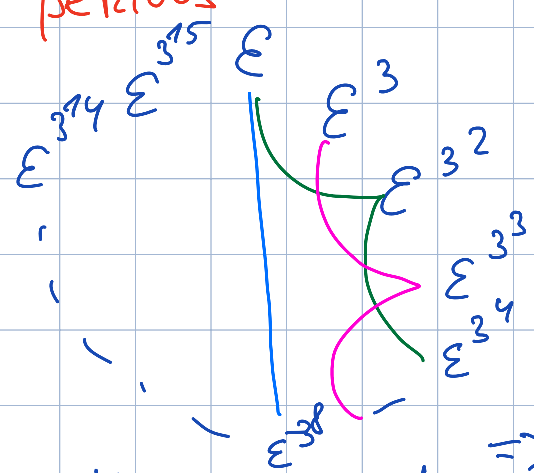
— — — — — — — — — — — — — —

For example, if $\alpha_0 = \alpha_1$, then $a_0 = \dots = a_{15} \Leftrightarrow \alpha_0 \in \mathbb{Q}$

Further $\alpha_0 = \alpha_2 \Leftrightarrow \begin{cases} a_0 = a_2 = a_4 = \dots \\ a_1 = a_3 = a_5 = \dots \end{cases} \Leftrightarrow \deg \alpha_0 \in \{1,2\}$

$\alpha_0 = \alpha_4 \Leftrightarrow \begin{cases} a_0 = a_4 = \dots \\ a_1 = a_5 = \dots \\ a_2 = a_6 = \dots \\ a_3 = a_7 = \dots \end{cases} \Leftrightarrow \deg \alpha_0 \in \{1,2,4\}$

Gauss periods



$\theta_0 = \theta_0(\varepsilon) = \varepsilon + \varepsilon^{3^2} + \dots + \varepsilon^{3^{14}}$

$\theta_1 = \theta_1(\varepsilon) = \varepsilon^3 + \varepsilon^{3^3} + \dots + \varepsilon^{3^{15}}$

Clearly, $\theta_0(\varepsilon^3) = \theta_1(\varepsilon)$ but, say, $\theta_0(\varepsilon^{3^2}) = \theta_0(\varepsilon)$

$\Rightarrow \theta_0$ & θ_1 are roots of a quadratic equation (e.g. $\theta_0 + \theta_1 = -1$)

Thus we put $K_1 = \mathbb{Q}(\theta_0, \theta_1) = \mathbb{Q}(\theta_0) = \mathbb{Q}(\theta_1)$

Further $\theta_{00} = \varepsilon + \varepsilon^{3^4} + \varepsilon^{3^8} + \varepsilon^{3^{12}}$ and so on.

E.g. $\theta_{00} + \theta_{01} = \theta_0$, $\theta_{10} + \theta_{11} = \theta_1$

Finally, $\theta_{000} = \varepsilon + \varepsilon^{3^8} = \varepsilon + \varepsilon^{-1} = 2\cos\frac{2\pi}{17}$

Put $K_2 = \mathbb{Q}(\theta_{00})$, $K_3 = \mathbb{Q}(\theta_{000})$

Unfortunetly, it is not obvious that $K_1 \subseteq K_2 \subseteq K_3$

On the other hand, there are vector spaces

$\mathbb{Q} = V_1 : a_0 = \ldots = a_{15}$

$V_2 : \begin{cases} a_0 = a_2 = a_4 = \ldots \\ a_1 = a_3 = a_5 = \ldots \end{cases}$

$V_4 : \begin{cases} a_0 = a_4 = \ldots \\ a_1 = a_5 = \ldots \\ a_2 = a_6 = \ldots \\ a_3 = a_7 = \ldots \end{cases}$ and, similarly, V_8 and $V_{16} = \mathbb{Q}(\varepsilon)$

Now it is obvious that $\underset{\mathbb{Q}}{\underset{\|}{V_1}} \subset \underset{\mathbb{Q}(\theta_0)}{\underset{\|}{V_2}} \subset V_4 \subset V_8 \subset V_{16}$

But V_j are vector spaces, not fields. It is enough to obtain:

L. $\forall d$, $\forall d$-period θ one has $V_d = \mathbb{Q}(\theta)$.

Pf. We have $\dim_{\mathbb{Q}} V_d = d$ and $\dim_{\mathbb{Q}} \mathbb{Q}(\theta)$ $=$ # conjugates of $\theta = d$. Also, we know that $V_d = \{\alpha \in \mathbb{Q}(\varepsilon) \mid \deg \alpha \mid d\}$, $d = 1, 2, 4, 8, 16$.

Finally, $\mathbb{Q}(\theta) = \{h(\theta) \mid h \in \mathbb{Q}[x]\}$.

$$\underbrace{\mathbb{Q} - \mathbb{Q}(f(\theta)) - \mathbb{Q}(\theta)}_{d}$$ $\Rightarrow$ by the tower law one has $\deg f(\theta) \mid d$

Thus $\mathbb{Q}(\theta) \subseteq V_d \Rightarrow \mathbb{Q}(\theta) = V_d$. ∎