6 Compass-ruler (Straightedge) Construction

Historical problems of Compass-ruler construction

① trisect an arbitary angle (✗)

② a cube with its volume twice as a known one (✗)

③ a square with the area equal to a known circle (✗)

④ what kind of regular polygons can be constructed ? (✓✗)

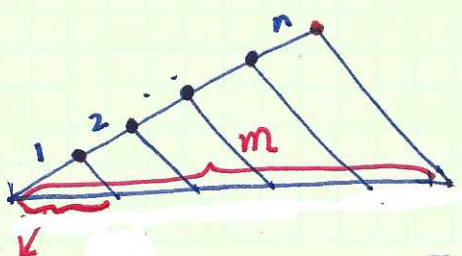
Since a Compass and a ruler can only plot a straight line and circle:

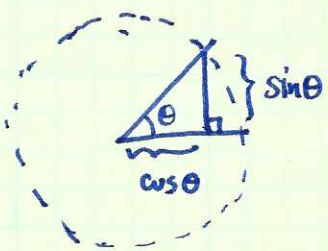
$$\begin{cases} y = kx + b \\ x^2 + y^2 + cx + dy = e \end{cases}$$

They are just linear and quardartic equations. Hence, the solutions can only be based on the known quantities (coefficients) via $+ - \times \div$ and $\sqrt{}$.

Hence the problem that a quantity can be constructed by Compass-rule if is equivalent to if such a quantity can be obtained via field extension based on taking square root.

Let us denote the number field avaible at the beginning as F. It can be based on a length unit, then it is easy to reach $\mathbb{Q}$. We may be given an angle θ, which means $\cos\theta$ or $\sin\theta$ are added into $\mathbb{Q}$, if they are not rational. Let us call this number field as F. This is our starting point.





$$F = \mathbb{Q}(\cos\theta, \sin\theta)$$

By ruler-compass, we can only add $\sqrt{a}$, $\sqrt{b}$, etc to F, hence the extended field $K = F(\sqrt{a}, \sqrt{b}, \cdots)$. It's dimension relative to F must be a power of 2, i.e. $\boxed{[K:F] = 2^m}$.

Theorem: if $p(x)$ is an irreducible cubic polynomial on F, and K is F's extended field with $[K:F] = 2^m$, then $p(x)$ remains irreducible on K.

Proof: If $p(x)$ is reducible on K then $p(x) = p_1(x)\,p_2(x)$, and one of them must be linear, say, $p_1(x) = x - u$. Then $u \in K$, but $u \notin F$. Hence $F \subset F(u) \subset K$. Then we assume $p(x) = a_3x^3 + a_2x^2 + a_1x + a_0 = 0$, ($a_{1,2,3,0} \in F$)

Since it's irreducible, $F(u)$ can be represented as

$$h_0 + h_1u + h_2u^2, \text{ with } h_{0,1,2} \in F.$$

i.e. $[F(u):F] = 3$, hence $3 \nmid 2^m$, which is impossible.

(*) Now we prove the impossibility of trisecting an angle.

$$\cos\theta = 4\cos^3\frac{\theta}{3} - 3\cos\frac{\theta}{3} \qquad \text{set } a = \cos\theta,\ x = \cos\theta/3$$

$$\Rightarrow 4x^3 - 3x = a \quad \text{or} \quad \boxed{x^3 - \tfrac{3}{4}x - \tfrac{a}{4} = 0}$$

$$\Delta = \left(\tfrac{1}{2}(-\tfrac{a}{4})\right)^2 + \left(\tfrac{1}{3}\tfrac{-3}{4}\right)^3 = \frac{1}{64}(-1+a^2) = \frac{-1}{64}\sin^2\theta$$

$$\sqrt{\Delta} = \sqrt{-1}/8\,\sin\theta, \text{ we can add } \sqrt{-1}\sin\theta \text{ into F as}$$

$$F(\cos\theta, \sqrt{-1}\sin\theta) = F(\cos\theta, \sqrt{\cos^2\theta - 1}).$$

All these kind of extensions changes the dimesion by 2^m.

multipling

Now according to a previous theorem, the roots $x_1\ x_2\ x_3$ either all of them belong to a further extension $F' = F(a, \sqrt{a^2-1}, y_1)$, or, none of them belong to F'. Hence, $x^3 - \frac{3}{4}x - \frac{a}{4}$ on the field $F(a, \sqrt{a^2-1}, y)$ either completely reducible $(x-x_1)(x-x_2)(x-x_3)$, or, irreducible.

Unless, for a special value of $a = \cos\theta$, such that $x^3 - \frac{3}{4}x - \frac{a}{4}$ is completely reducible, the minimum extension F', satisfies

$$[F' : F(a, \sqrt{a^2-1})] = 3.$$

But $[K : F] = 2^m$, Hence, $F' \not\subset k$, $\Rightarrow$ $x^3 - \frac{3}{4}x - \frac{a}{4}$ remains ireducible on K.

(*) Obviously $[Q(\sqrt[3]{2}) : Q] = 3$, $\sqrt[3]{2}$ cannot be ~~constructed~~ !

(*) π is a transcidental number, which cannot be ~~constructed~~, either. The proof is beyond the scope of this note!

• Compass and ruler construction for regular polygons?

① It's obvious that 2^m (regular) polygons can be constructed.

② what kind of odd prime number p that the p-regular-polygon can be constructed?

This is equivalent to the problem that if $Q(\zeta_p)/Q$ can be extented via taking $\sqrt{\ }$. We have known it's a $p-1$th order cyclic extension. Hence, we need $p-1 = 2^l$. If l has an odd factor $l = p_1 p_2$ that p_1 is odd, then $p = (2^{p_2})^{p_1} + 1 = (2^{p_2}+1)((2^{p_2})^{p_1-1} - (2^{p_2})^{p_1-2} + \dots)$. It cannot be a prime number, hence $l = 2^t \Rightarrow$ P should be a Fermat type prime number, $p = 2^{2^t} + 1 = F_t$.

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65,537$, but $F_{5,6}$ are not prime numbers any more.

③ How about p^α - regular polygons?

Then the unit root ζ_{p^α}, — extension to Q; $\varphi(p^\alpha) = p^\alpha(1 - 1/p)$ $= p^{\alpha-1}(p-1)$. if $\alpha \geq 1$, it is impossible that $2^m \mid p^{\alpha-1}(p-1)$, hence $\alpha = 1$.

④ If for $n = 2^m, p_1, \dots, p_s$, the regular polygens can be constructed, then any-product polygens of can also be constructed.

Proof: All these numbers do not have common prime factor.

Say if n_1 and n_2 can be constructed, and they are products without overlapping prime factors, then $(n_1, n_2) = 1$. Then there must be integers r and s, such that $rn_1 + sn_2 = 1$, $\Rightarrow 2\pi\left(\frac{r}{n_2} + \frac{s}{n_2}\right) = \frac{2\pi}{n_1 n_2}$.

(r, or, s, may be negative.). Then we can construct $\frac{2\pi}{n_1}$ - $|r|$-times, and $2\pi/n_2$ · s-times, and take their difference.

Now we have the following theorem (Gauss). The regular n-polygens can be constructed by compass and ruler iff $n = 2^s P_1 P_2 \cdots P_s$, and $P_i = 2^{2^t} + 1$, i.e. Fermat type prime number.

- Gauss's solution to the construction of regular 17-polygen

Define $\xi = e^{i\frac{2\pi}{17}}$. Consider the mapping $\sigma(\xi) = \xi^3$, and use this as a generator to generate the 16-th cyclic group.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\sigma^n(\xi)$	ξ	ξ^3	ξ^9	ξ^{10}	ξ^{13}	ξ^5	ξ^{15}	ξ^{11}	ξ^{16}	ξ^{14}	ξ^8	ξ^7	ξ^4	ξ^{12}	ξ^2	ξ^6

Then the field extension processes are

$$F_1 = \mathbb{Q} \longrightarrow F_2 = \mathbb{Q}(\eta_2) \longrightarrow F_3 = F_2(\eta_3) \longrightarrow F_4 = F_3(\xi + \xi^{-1}) \longrightarrow N = F_4(\xi)$$

① $\mathrm{Gal}(F_2/F_1) = \langle\sigma\rangle/\langle\sigma^2\rangle = \{1, \sigma\}$ ← coset between Z_{16}/Z_8

Adel $\eta_2 = \sum_{i=0}^{7} \sigma^{2i}(\xi) = \xi + \xi^9 + \xi^{13} + \xi^{15} + \xi^{16} + \xi^8 + \xi^4 + \xi^2$

and $\sigma(\eta_2) = \xi^3 + \xi^{10} + \xi^5 + \xi^{11} + \xi^{14} + \xi^7 + \xi^{12} + \xi^6$

(1) $Gal(N/F_1) = \{\sigma\}$, $Gal\{N/F_2\} = \{\sigma^2\}$

η_2 and $\sigma(\eta_2) \in F_2$, but not in F_1; they belong $\sqrt{\ }$ extension. They are invariant under σ^2.

$$\begin{cases} \eta_2 + \sigma(\eta_2) = -1 \\ \eta_2 \cdot \sigma(\eta_2) = 4(\xi^1 + \cdots \xi^{16}) = -4 \end{cases} \Rightarrow \eta_2 = \frac{-1+\sqrt{17}}{2} > 0$$

$$\sigma(\eta_2) = \frac{-1-\sqrt{17}}{2} < 0.$$

(2) $Gal(N/F_3) = \langle \sigma^4 \rangle$, $Gal(N/F_2) = \langle \sigma^2 \rangle$

$\Rightarrow Gal(F_3/F_2) = \langle \sigma^2 \rangle / \langle \sigma^4 \rangle$, i.e. we need to find a # invariant under σ^4, i.e $\sigma^4(\eta_3) = \eta_3$ but $\sigma^2(\eta_3) \neq \eta_3$.

Consider $\eta_3 = \sigma^0(\xi) + \sigma^4(\xi) + \sigma^8(\xi) + \sigma^{12}(\xi)$

$$= \xi + \xi^{13} + \xi^{16} + \xi^4 = \xi + \xi^{-1} + \xi^4 + \xi^{-4}$$

$$\sigma^2(\eta_3) = \sigma^2(\xi) + \sigma^6(\xi) + \sigma^{10}(\xi) + \sigma^{14}(\xi)$$

$$= \xi^9 + \xi^{15} + \xi^8 + \xi^2 = \xi^2 + \xi^{-2} + \xi^8 + \xi^{-8}$$

$$\Rightarrow \begin{cases} \eta_3 + \sigma^2(\eta_3) = \eta_2 \\ \eta_3 \cdot \sigma^2(\eta_3) = \xi^3 + \xi^{-1} + \xi^9 + \xi^{-7} + \xi^1 + \xi^{-3} + \xi^7 + \xi^{-9} \\ \quad + \xi^6 + \xi^2 + \xi^{12} + \xi^{-4} + \xi^{-2} + \xi^{-6} + \xi^4 + \xi^{-12} \\ \quad = \xi^1 + \cdots \xi^{16} = -1 \end{cases} \quad \eta_3 = \frac{\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}}}{4}$$

$$\Rightarrow \eta_3 = \frac{\eta_2 + \sqrt{\eta_2^2 + 4}}{2} > 0 \qquad \sigma^2(\eta_3) = \frac{\eta_2 - \sqrt{\eta_2^2+4}}{2} < 0$$

Then $Gal(F_3/F_1) = \langle \sigma \rangle / \langle \sigma^4 \rangle$ — 4th order extension

$$\sigma(\eta_3) = \frac{\sigma(\eta_2) + \sqrt{(\sigma(\eta_2))^2 + 4}}{2} = \frac{-(\sqrt{17}+1) + \sqrt{34+2\sqrt{17}}}{4}$$

$$\sigma^3(\eta_3) = \sigma(\sigma^2(\eta_3)) = \frac{\sigma(\eta_2) - \sqrt{\sigma(\eta_2)^2 + 4}}{2}$$

③ $\mathrm{Gal}(N/F_4) = \langle \sigma^8 \rangle$ $\quad \mathrm{Gal}(N/F_3) = \langle \sigma^4 \rangle$

$\Rightarrow \mathrm{Gal}(F_4/F_3) = \langle \sigma^4 \rangle / \langle \sigma^8 \rangle$.

Find η_4 such that $\sigma^8(\eta_4) = \eta_4$, but $\sigma^4(\eta_4) \neq \eta_4$.

$$\eta_4 = \sigma^0(\zeta) + \sigma^8(\zeta) = \zeta + \zeta^{-1}$$

$$\sigma^4(\eta_4) = \sigma^4(\zeta) + \sigma^{12}(\zeta) = \zeta^{13} + \zeta^4 = \zeta^4 + \zeta^{-4}$$

Again $\eta_4 + \sigma^4(\eta_4) = \eta_3$

$$\eta_4 \cdot \sigma^4(\eta_4) = \zeta^5 + \zeta^{-3} + \zeta^3 + \zeta^{-5} = \zeta^3 + \zeta^{-3} + \zeta^5 + \zeta^{-5} = \sigma(\eta_3)$$

$$\Rightarrow \eta_4 = \zeta + \zeta^{-1} = \frac{1}{2}\left(\eta_3 + \sqrt{\eta_3^2 - 4\sigma(\eta_3)}\right) \qquad (\eta_4 > \sigma^4(\eta_4)).$$

$$\sigma^4(\eta_4) = \zeta^4 + \zeta^{-4} = \frac{1}{2}\left(\eta_3 - \sqrt{\eta_3^2 - 4\sigma(\eta_3)}\right)$$

$$\Rightarrow \cos\frac{2\pi}{17} = \frac{\eta_4}{2} = \frac{1}{4}\left(\eta_3 + \sqrt{\eta_3^2 - 4\sigma(\eta_3)}\right)$$

$$\eta_3 = \frac{\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}}}{4}$$

$$\sigma(\eta_3) = \frac{-(\sqrt{17}+1) + \sqrt{34 + 2\sqrt{17}}}{4}$$

↘ every square root can be constructed, hence $\cos\frac{2\pi}{17}$ can also be constructed!