## Lecture 5 : Ruler and Compass Constructions II

---

### Objectives

(1) Wantzel's characterization of constructible regular $p$-polygons.
(2) Richmond's construction of a regular pentagon.
(3) Gauss' criterion of constructible regular polygons.

**Key words and phrases:** Fermat's primes, constructible regular polygons, Gauss' criterion.

---

In this section we discuss constructibility by ruler and compass of regular polygons. Gauss' proved that a regular polygon of $n$ sides is constructible by ruler and compass if and only if $n = 2^m p_1 p_2 \dots p_r$ where $m \in \mathbb{N}$ and $p_1, p_2, \dots, p_r$ are distinct Fermat primes. The number $F_m = 2^{2^m} + 1$ is called a **Fermat prime** whenever it is a prime. The known Fermat primes are:

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257 \text{ and } F_4 = 65537.$$

Fermat showed that $F_m$ is a prime for $m \leq 4$. Eisenstein conjectured that there are infinitely many Fermat primes. This conjecture is still open. Euler showed that $F_5$ is divisible by 641.

**Proposition 5.1** (1837, Wantzel)**.** *Let a regular polygon of $n$ sides be constructible and $p$ be an odd prime dividing $n$. Then $p$ is a Fermat prime.*

*Proof.* If $p|n$ and a regular $n$-gon is constructible then a regular $p$-gon is also constructible. Thus the point $(\cos 2\pi/p, \sin 2\pi/p)$ is a constructible point. Hence there exists a field $F \supseteq \mathbb{Q}$ such that $[F : \mathbb{Q}] = 2^m$ and $\cos 2\pi/p, \sin 2\pi/p \in F$. Then $\zeta_p = \cos 2\pi/p + i \sin 2\pi/p \in F(i)$ and hence $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = 2^s = p - 1$ and therefore $p = 1 + 2^s$. It follows that $s$ is a power of 2. Hence $p$ is a Fermat prime. $\square$

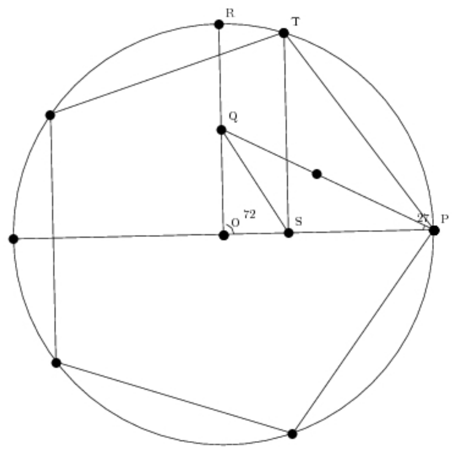


FIGURE 1. Richmond's construction of a regular pentagon

**Construction of a pentagon by ruler and compass**

We show that a pentagon is constructible by ruler and compass. The vertex $(\cos 72^0, \sin 72^0)$ of a regular pentagon corresponds to the complex number $z = e^{2\pi i/5}$ which is the root of the irreducible polynomial

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1.$$

Therefore

$$z^2 + z + 1 + \frac{1}{z} + \frac{1}{z^2} = 0.$$

Completing the square we get

$$\left(z + \frac{1}{z}\right)^2 + \left(z + \frac{1}{z}\right) - 1 = 0.$$

Put $z + 1/z = y$ to get $y^2 + y - 1 = 0$ and $z^2 - zy + 1 = 0$. Hence $y = (-1 \pm \sqrt{5})/2$. The second equation gives $z = (y \pm \sqrt{y^2 - 4})/2$. Clearly $y$ is constructible as it belongs to $\mathbb{Q}(\sqrt{5})$ and we have a square root tower

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt{5}, \sqrt{y^2 - 4}).$$

Thus all roots of $\Phi_5(x)$ are constructible real numbers.

**Richmond's construction of a regular pentagon (1893)**

Draw a unit circle with center $O$. Draw a perpendicular $OR$ at $O$. Let $Q$ be the mid point of $OR$. Join $Q$ and $P$ and then bisect $\angle PQO$. Let the bisector meet $OP$ at $S$. Construct a perpendicular at $S$ and let $T$ be its intersection point with the circle. We show $\angle TOP = 72^o$. It is enough to show that $OS = \cos 72^o$. Note that

$$\angle OQS = \tfrac{90-\theta}{2} \Rightarrow \tan\left(45^o - \tfrac{\theta}{2}\right) = \tfrac{OS}{\frac{1}{2}} \Rightarrow OS = \tfrac{1}{2}\tan(45^o - \tfrac{\theta}{2}).$$

Using $\tan\theta = \frac{1}{2} = \frac{2\tan\theta/2}{1-\tan^2\theta/2}$ we get $\tan\frac{\theta}{2} = \sqrt{5}-2$. Therefore

$$OS = \tfrac{1}{2}\left(\tfrac{\tan 45^o - \tan\theta/2}{1-\tan 45^o \tan(-\theta/2)}\right) = \tfrac{\sqrt{5}-1}{4} = \cos 72^o.$$

**Proposition 5.2.** *A heptagon is not constructible by ruler and compass.*

*Proof.* Let $\theta = 2\pi/7$ and $\zeta_7 = \cos\theta + i\sin\theta$. Then $\zeta_7$ is a root of the irreducible polynomial

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Therefore $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$. Using $\zeta_7 + \overline{\zeta_7} = 2\cos\theta$ we get $[\mathbb{Q}(\zeta_7) : \mathbb{Q}(\cos\theta)] = 2$ and hence $[\mathbb{Q}(\cos\theta) : \mathbb{Q}] = 3$. Thus $\cos\theta$ is not constructible. Therefore a heptagon is not constructible by ruler and compass. $\square$

**Proposition 5.3.** *Let $p$ be a prime number and $\zeta_p = \cos 2\pi/p^2 + i\sin 2\pi/p^2$. Then*

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p(p-1).$$

*Proof.* Since $\zeta_p$ satisfies the equation

$$x^{p^2} - 1 = (x^p - 1)(x^{p(p-1)} + x^{p(p-2)} + \cdots + (x^p)^2 + x^p + 1) = 0$$

and $\zeta_p^p \neq 1$, $\zeta_p$ is root of $f(x) = (x^p)^{p-1} + (x^p)^{p-2} + \cdots + (x^p)^2 + x^p + 1$. We show that $f(x) \in \mathbb{Q}[x]$ is irreducible. Put $x = u+1$ and use Eisenstein's criterion:

$$\begin{aligned} f(u+1) &= \sum_{k=1}^{p}(u+1)^{p(p-k)} \\ &= \sum_{k=1}^{p}(u^p+1+pg(u))^{p-k} \\ &= \sum_{k=1}^{p}(u^p+1)^{p-k}+ph_k(u) \end{aligned}$$

where $h_k(u) \in \mathbb{Z}[u]$ has degree $p^2-pk-1$. Since

$$\textstyle\sum_{k=1}^{p}(u^2+1)^{p-k} = \frac{(u^p+1)^p-1}{u^p} = u^{p(p-1)}+pH(u),$$

$$f(u+1) = \sum_{k=1}^{p}(u+1)^{p(p-k)} = u^{p(p-1)}+pG(u).$$

Since $f(1)=p$, the constant term of $f(u+1)$ is divisible by $p$ and not by $p^2$. By Eisenstein's criterion $f(u+1)$ and hence $f(x)$ is irreducible. Thus $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p^2-p$. □

**Theorem 5.4** (Gauss)**.** *If a regular polygon of $n$ sides is constructible then $n = 2^r p_1 p_2 \ldots p_s$ where $p_1, \ldots, p_s$ are distinct Fermat primes.*

*Proof.* If $p^2 n$ then $p$-gon is constructible. Hence $[\mathbb{Q}(\cos 2\pi/p^2):\mathbb{Q}] = 2^u$ for some positive integer $u$. Thus $p(p-1) = 2^u$, which is a contradiction. □

This finishes the proof of one half of Gauss's constructibility criterion for regular polygons. We shall prove the other half after we prove the fundamental theorem of Galois Theory.