Fields and Galois Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

1. Regular Polygons
   - Preliminaries
   - The Construction of Regular Polygons

Subsection 1

Preliminaries

Closure Properties of Constructible Points

- Recall that a point (a,b) is **constructible** if it can be obtained from $O=(0,0)$ and $I=(1,0)$ by ruler and compasses constructions.

Lemma

Let $a,b\in\mathbb{R}$.

(i) The point $(a,0)$ is constructible if and only if $(0,a)$ is constructible.

(ii) The point (a,b) is constructible if and only if $(a,0)$ and $(b,0)$ are constructible.

(iii) If $(a,0)$ and $(b,0)$ are constructible, then so are $(a+b,0),(a-b,0),(ab,0)$ and, if $b\neq 0$, $(\frac{a}{b},0)$.

(i) Suppose that $(a,0)$ is constructible. The circle with center O passing through $(a,0)$ meets the positive y-axis in $(0,a)$. So $(0,a)$ is constructible. The converse is similar.

Closure Properties of Constructible Points (ii)

(ii) Suppose that (a, b) is constructible.
- We can drop a perpendicular from (a, b) on to the x-axis to construct the point $(a, 0)$.
- Dropping a perpendicular on to the y-axis gives the point $(0, b)$.

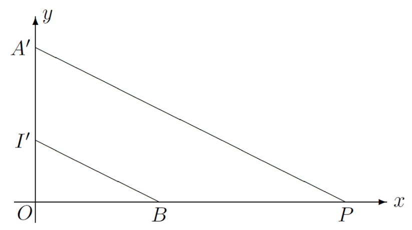
So, by Part (i), both $(a, 0)$ and $(b, 0)$ are constructible.

Conversely, suppose that $(a, 0)$ and $(b, 0)$ (and hence also $(0, b)$) are constructible.
- We may draw a line through $(a, 0)$ perpendicular to the x-axis.
- We may draw a line through $(0, b)$ perpendicular to the y-axis.

The lines meet in (a, b), which is therefore constructible.

Closure Properties of Constructible Points (iii)

(iii) Suppose that $A=(a,0)$ and $B=(b,0)$ are constructible. A circle with center A and radius equal to the length of OB meets the x-axis in $(a+b,0)$ and $(a-b,0)$. Hence, both these points are constructible.
We now show that $(ab,0)$ is constructible.
Let $A'=(0,a)$ and $I'=(0,1)$, both constructible, by Part (i).

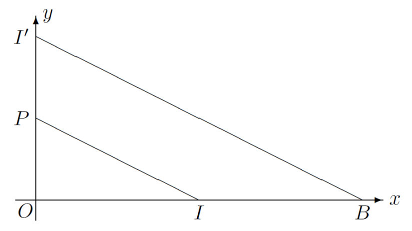


Draw a line though A' parallel to $I'B$, meeting the x-axis in P.
The triangles OBI' and OPA' are similar. So we have $\frac{OP}{OA'}=\frac{OB}{OI'}$.
Hence, P is the point $(ab,0)$. So it is constructible.

Closure Properties of Constructible Points (iii Cont'd)

- Finally, we show that $(\frac{a}{b}, 0)$ is constructible.

  Let B be the point $(b, 0)$, where $b \neq 0$, and let $I' = (0, 1)$.



  Draw a line through I parallel to BI', meeting the y-axis in P.

  The triangles OIP and OBI' are similar. So we have $\frac{OP}{OI} = \frac{OI'}{OB}$.

  Thus, P is the point $(0, \frac{1}{b})$. So $(\frac{1}{b}, 0)$ is also constructible.

  From the preceding result, we deduce that $(\frac{a}{b}, 0)$ is constructible.

Constructibility of Rational Pairs

Corollary

If $a, b \in \mathbb{Q}$, then (a, b) is constructible.

- From Part (iii) of the lemma, we can deduce that $(\frac{m}{n}, 0)$ is constructible for every rational number $\frac{m}{n}$.

  Thus, by Part (i), $(a,0)$ and $(0, b)$ are constructible.

  So, by Part (ii), (a, b) is constructible.

Constructibility Theorem

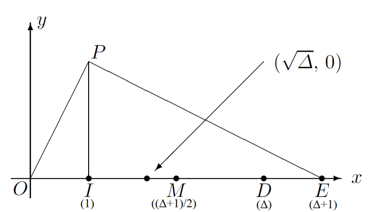
Theorem

Let $B = \{O, I\}$. If there is a sequence of subfields $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n = L$ of $\mathbb{R}$, such that $[K_i : K_{i-1}] = 2$, $i = 1, 2, \ldots, n$, then every point with coordinates in L is constructible.

- By the corollary, every (a, b) with coordinates in $\mathbb{Q} = K_0$ is constructible. Let $i \geq 1$. Suppose inductively that every point with coordinates in K_{i-1} is constructible. By hypothesis, $[K_i : K_{i-1}] = 2$. So $K_i = K_{i-1}(\beta)$, where β is an arbitrarily chosen element of $K_i \backslash K_{i-1}$. The minimum polynomial of β over K_{i-1} is of the form $X^2 + bX + c$, with $b, c \in K_{i-1}$. Its discriminant $\Delta = b^2 - 4c \geq 0$, since K_i is certainly a subfield of $\mathbb{R}$. Then $\beta = \frac{1}{2}(b \pm \sqrt{\Delta})$. So $K_i = K_{i-1}(\sqrt{\Delta})$, where $\Delta \in K_{i-1}$. It suffices to show that $(\sqrt{\Delta}, 0)$ is constructible.

Constructibility of $(\sqrt{\Delta},0)$

- Let D be the point $(\Delta,0)$. Let E be the point on the x-axis such that $IE=\Delta$. Let M be the midpoint of OE. Let $\mathscr{K}$ be the circle with center M passing through O (and E).
  Let the line through I perpendicular to the x-axis meet the circle $\mathscr{K}$ in P.



  The angle OPE is a right angle.

  The triangles OIP and PIE are similar. Hence, $\frac{OI}{IP}=\frac{IP}{IE}$. So $IP^2=\Delta$.

  The point $(\sqrt{\Delta},0)$ is obtained as the intersection with the positive x-axis of a circle with center O and radius equal to the length IP.

  It follows that an arbitrary point $(p+q\sqrt{\Delta},r+s\sqrt{\Delta})$, where $p,q,r,s\in K_{i-1}$, is constructible.

Extensions of $\mathbb{Q}$ of Degree a Power of 2

Theorem

Let K be a normal extension of $\mathbb{Q}$, such that $[K:\mathbb{Q}] = 2^m$, where m is a positive integer. Then, every point (α, β) in $K \times K$ is constructible.

- The group $G = \mathrm{Gal}(K:\mathbb{Q})$ is of order 2^m. By a preceding theorem, there exist normal subgroups

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_{m-1} \subset H_m = G,$$

such that $|H_i| = 2^i$, $i = 0, 1, \ldots, m$. Thus, there exist subfields

$$K = \Phi(H_0) \supset \Phi(H_1) \supset \cdots \supset \Phi(H_{m-1}) \supset \Phi(H_m) = \mathbb{Q},$$

with $[K : \Phi(H_i)] = 2^i$, $i = 0, 1, \ldots, m$.
Hence, $[\Phi(H_i) : \Phi(H_{i+1})] = 2$, $i = 0, 1, \ldots, m-1$.
The conclusion now follows from the preceding theorem.

Subsection 2

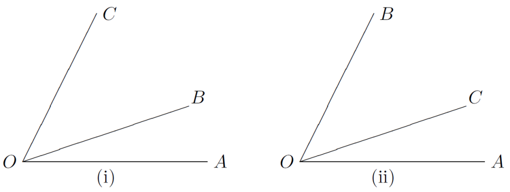
The Construction of Regular Polygons

Construction of the Canonical n-Gon

- For all $n \geq 3$, denote the regular polygon with n sides by Π_n.
- We specify exactly the set of n for which Π_n is constructible.
- The key is that a geometric construction is possible if and only if the degree of the associated field extension is a power of 2.
- Note, first, that the construction of Π_n depends on the construction of the angle $\theta_n = \frac{2\pi}{n}$ at the center of the polygon
- Once we construct the isosceles triangle IOA for which the angle IOA is θ_n, we may form the polygon by pasting copies of the triangle all the way round.

Sum/Difference of Constructible Angles

- A similar pasting technique allows us to deduce that constructibility of θ_m and θ_n implies constructibility of $\theta_m \pm \theta_n$.



- In both diagrams, AOB is the angle θ_m.
  - In (i), $\angle BOC = \theta_n$ and $\angle AOC = \theta_m + \theta_n$.
  - In (ii), $\angle COB = \theta_n$ and $\angle AOC = \theta_m - \theta_n$.

Theorem

If θ_m and θ_n are constructible and $s, t \in \mathbb{Z}$, then $s\theta_m + t\theta_n$ is constructible.

Constructibility of an Angle

Theorem

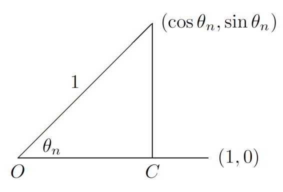
The following statements are equivalent:

(i) θ_n is constructible;

(ii) The point $(\cos\theta_n, \sin\theta_n)$ is constructible;

(iii) The point $(\cos\theta_n, 0)$ is constructible.

(i)⇒(ii): This is clear from the diagram:



(ii)⇒(iii): This is clear from the preceding lemma.

(iii)⇒(i): In the diagram, suppose we have constructed the point $C(\cos\theta_n, 0)$. The line though C perpendicular to OI meets the circle with center O and radius 1 in the point $(\cos\theta_n, \sin\theta_n)$. Joining this point to O gives the required angle.

Constructibility of Π_{mn} from Π_m and Π_n

Lemma

Let m and n be relatively prime positive integers. Π_{mn} is constructible if and only if Π_m and Π_n are constructible.

- Suppose first that Π_{mn}, with vertices $V_0, V_1, \ldots, V_{mn-1}$, is constructible. It is clear that Π_m is constructible. Simply join up the vertices $V_0, V_n, V_{2n}, \ldots, V_{(m-1)n}, V_0$ in sequence. Similarly, Π_n is constructible.

  Note that "relatively prime" was not used in this part of the proof.

  Conversely, suppose that Π_m and Π_n are constructible, where m and n are relatively prime. Then, there exist integers s and t, such that $sm + tn = 1$. So

$$s\theta_n + t\theta_m = \frac{2\pi s}{n} + \frac{2\pi t}{m} = \frac{2\pi(sm+tn)}{mn} = \theta_{mn}.$$

  By a previous theorem, $s\theta_n + t\theta_m$ is constructible. Thus, so is θ_{mn}.

Constructibility of θ_p

Lemma

Let $\omega_p = e^{\theta_p} = e^{2\pi i/p}$, where p is prime. Then θ_p is constructible if and only if $[\mathbb{Q}(\omega_p) : \mathbb{Q}]$ is a power of 2.

- Let $\omega = e^{2\pi i/p}$. Over the field $\mathbb{Q}(\omega)$ the polynomial $X^p - 1$ factorizes as $(X-1)(X-\omega)(X-\omega^2)\cdots(X-\omega^{p-1})$. So $\mathbb{Q}(\omega)$ is the splitting field over $\mathbb{Q}$ of the polynomial $\frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + X + 1$. The polynomial is irreducible over $\mathbb{Q}$. $\mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$ is abelian. Let $K = \mathbb{Q}(\omega) \cap \mathbb{R}$. This is a subfield of $\mathbb{R}$ containing $\zeta = \frac{\omega+\omega^{-1}}{2} = \cos\frac{2\pi}{p}$. The minimum polynomial of ω over K is $X^2 - 2\zeta X + 1$. So $[\mathbb{Q}(\omega) : K] = 2$. Hence, $\mathrm{Gal}(\mathbb{Q}(\omega) : K)$ is a subgroup of $\mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$ of order 2. It is a normal subgroup, since $\mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$ is abelian. Hence, the extension $K : \mathbb{Q}$ is normal. By preceding results, $\frac{2\pi}{p}$ is constructible if and only if $[K : \mathbb{Q}]$ is a power of 2. Hence, (since $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2[K : \mathbb{Q}]$) if and only if $[\mathbb{Q}(\omega) : \mathbb{Q}]$ is a power of 2.

Minimum Polynomial of Primitive Roots

- Let p be a prime, $q = p^m$ and $\omega \in \mathbb{C}$ a **primitive** q-th root of unity, i.e., $\omega^{p^m} = 1$, but $\omega^{p^{m-1}} \neq 1$.

Lemma

The minimum polynomial of ω is $f = 1 + X^{p^{m-1}} + X^{2p^{m-1}} + \cdots + X^{(p-1)p^{m-1}}$.

- Write $X^{p^{m-1}}$ as Z. Then

$$f = 1 + Z + \cdots + Z^{p-1} = \frac{Z^p - 1}{Z - 1} = \frac{X^{p^m} - 1}{X^{p^{m-1}} - 1}.$$

We have $f(\omega) = 0$. It remains to show that f is irreducible over $\mathbb{Q}$.

Let $X = 1 + T$. Then $f = \frac{(1+T)^{p^m} - 1}{(1+T)^{p^{m-1}} - 1}$.

All the intermediate binomial coefficients are divisible by p.

So we may write $f = \frac{T^{p^m} + pu(T)}{T^{p^{m-1}} + pv(T)}$, where u and v are polynomials, and $\partial u \leq p^m - 1$, $\partial v \leq p^{m-1} - 1$.

Minimum Polynomial of Primitive Roots (Cont'd)

- We now have

$$\begin{aligned} f &= \frac{(1+T)^{p^m}-1}{(1+T)^{p^{m-1}}-1} \\ &= \frac{T^{p^m}+pT^{p^{m-1}(p-1)}v(T)-pT^{p^{m-1}(p-1)}v(T)+pu(T)}{T^{p^{m-1}}+pv(T)} \\ &= \frac{T^{p^{m-1}(p-1)}(T^{p^{m-1}}+pv(T))-pT^{p^{m-1}(p-1)}v(T)+pu(T)}{T^{p^{m-1}}+pv(T)} \\ &= T^{p^{m-1}(p-1)}+\frac{pu(T)-pT^{p^{m-1}(p-1)}v(T)}{T^{p^{m-1}}+pv(T)}. \end{aligned}$$

Minimum Polynomial of Primitive Roots (Cont'd)

- We got $f = T^{p^{m-1}(p-1)} + \frac{pu(T) - pT^{p^{m-1}(p-1)}v(T)}{T^{p^{m-1}} + pv(T)}$.

  The degree of the numerator $pu(T) - pT^{p^{m-1}(p-1)}$ is less than p^m.

  The degree of the denominator is p^{m-1}. f is a polynomial in T.

  The fractional term must be a polynomial of degree $< p^{m-1}(p-1)$.

  The numerator is divisible by p and the denominator is not.

  So we may write $f = T^{p^{m-1}(p-1)} + pg(T)$, where g is a polynomial and $\partial g < p^{m-1}(p-1)$. But we also have the expression

$$f(1+T) = 1 + (1+T)^{p^{m-1}} + (1+T)^{2p^{m-1}} + \cdots + (1+T)^{(p-1)p^{m-1}}.$$

  From this it is evident that the constant term of $f(1+T)$ is p.

  By Eisenstein's Criterion, $f = T^{p^{m-1}(p-1)} + pg(T)$ is irreducible.

Constructible Regular Polygons

Theorem

A regular polygon with n sides is constructible if and only if

$$n = 2^k p_1 p_2 \cdots p_r,$$

where k and r are non-negative integers and $p_1, p_2, \ldots, p_r$ are distinct prime numbers of the form $2^{2^m} + 1$.

- Let $n = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$, where $p_1, p_2, \ldots, p_s$ are distinct primes and $m_1, m_2, \ldots, m_s \geq 1$, and suppose that Π_n is constructible.
  By a previous lemma, Π_q is constructible, where $q = p^m$ is any of $p_j^{m_j}$.
  So the point $(\cos\theta_q, \sin\theta_q)$ is constructible, where $\theta_q = \frac{2\pi}{q}$.
  Hence, $[\mathbb{Q}(\cos\theta_q, \sin\theta_q) : \mathbb{Q}]$ is a power of 2.
  Also $\mathbb{Q}(\omega) = \mathbb{Q}(\cos\theta_q, \sin\theta_q, i) : \mathbb{Q}(\cos\theta_q, \sin\theta_q)$ is of degree 2.
  So $[\mathbb{Q}(\omega) : \mathbb{Q}]$ is also a power of 2.
  The complex number ω is a primitive q-th root of unity.

Constructible Regular Polygons (Cont'd)

- We know that $[\mathbb{Q}(e^{2\pi i/q}):\mathbb{Q}] = 2^r$, a power of 2.

  From the lemma, $[\mathbb{Q}(e^{2\pi i/q}):\mathbb{Q}] = p^{m-1}(p-1)$.
  - If $p=2$, no conflict occurs.
  - If p is odd, then $m=1$ and $p-1$ is a power of 2.

    Suppose that $p = 2^k+1$ and $k = 2^v u$, where $u>1$ is odd.

    Then, writing 2^{2^v} as w, we have

    $$\begin{aligned} p &= 2^{2^v u}+1 = (2^{2^v})^u+1 = w^u+1 \\ &= (w+1)(w^{u-1}-w^{u-2}+\cdots-w+1). \end{aligned}$$

    This is impossible, since p is prime.

    Hence, k has no odd factors.

    We conclude that p is a Fermat prime, of the form $2^{2^m}+1$.

  So, if Π_n is constructible, $n = 2^k p_1 p_2 \cdots p_r$, where each p_i is a Fermat prime.

Constructible Regular Polygons (Converse)

- Conversely, suppose that

$$n = 2^k p_1 p_2 \cdots p_r,$$

where each $p_j = 2^{2^{m_j}} + 1$ is a Fermat prime.

It suffices to show that Π_{2^k} and $\Pi_{p_j}, i = 1, 2, \ldots, r$, are constructible.

We can repeatedly bisect the angle $\frac{\pi}{2}$ to obtain $\frac{\pi}{2^{k-1}}$.

So Π_{2^k} is constructible.

We must show that each Π_{p_j} is constructible. Let $\omega = e^{2\pi i/p_j}$.

Then, by a previous lemma, $\mathbb{Q}(\omega)$ is a normal extension of $\mathbb{Q}$, with

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = p_j - 1 = 2^{2^{m_j}}.$$

Also by a previous lemma, the angle $\frac{2\pi i}{p_j}$ is constructible.