Lecture 17: Constructions by Straightedge and Compass

MAT205 Abstract Algebra II

Ma, Jia-Jun

Xiamen University Malaysia

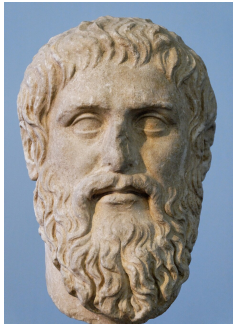
Part I: Constructible Numbers and the Field F

Doubling the Cube

The Delian altar (Plutarch, Eutocius). About 430 BC, plague on Delos; Apollo's oracle ordered the cubic altar doubled. The islanders doubled every edge—volume octupled, plague stayed. Plato told them the god wanted geometry, not arithmetic.

The problem. Given a segment of length 1, construct one of length $\sqrt[3]{2}$ by straightedge and compass.

Ancient workarounds. Hippocrates of Chios reduced this to finding two mean proportionals between 1 and 2; Menaechmus solved that with conics. Source: Eratosthenes' letter to Ptolemy III, lost itself but copied verbatim into Eutocius's commentary on Archimedes (c. 500 AD).



Plato (427–347 BC) Athenian philosopher; transmits the Delian story.

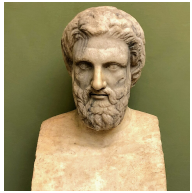
Squaring the Circle

Earliest traces. Anaxagoras, jailed in Athens for impiety (he taught that the sun was a hot stone), is said by Plutarch to have worked on squaring the circle in prison—the first written trace. Aristophanes' *Birds* (414 BC) sends Meton on stage with a ruler, promising to "make the circle square"—already a household joke.

The problem. Given the unit disk, construct a square of equal area—equivalently, $\sqrt{\pi}$—by straightedge and compass.

Hippocrates' lunes. Hippocrates of Chios squared certain crescents between two circular arcs—the first exact squaring of a curvilinear region. The method did not extend to the circle.

Anaxagoras (c. 500–428 BC)



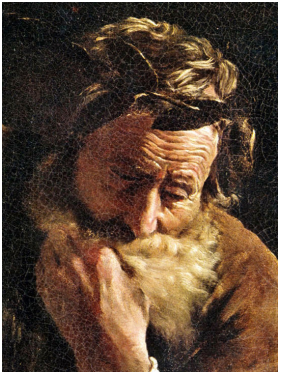
Aristophanes (c. 446–386 BC)

Trisecting the Angle

Ancient solutions. Hippias of Elis (c. 420 BC) invented the *quadratrix*, a curve that trisects any angle but is not itself constructible by line and circle. Archimedes added a clean *neusis* (marked-ruler) trisection—an extra rule, not a straightedge construction.

The problem. Given an angle θ, construct $\theta/3$ with straightedge and compass alone. Already 60° resists: trisecting it is the same as constructing $\cos 20^\circ$.

Classification (Pappus). The *Mathematical Collection* IV (c. 320 AD) classes such problems as "solid"—reachable with conics, suspected unreachable with line and circle. Wantzel (1837) proved the impossibility.



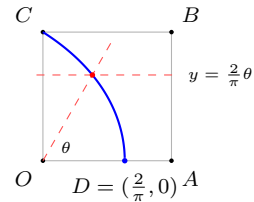
Archimedes (c. 287–212 BC)
Syracusan polymath;
exhaustion, π bounds;
neusis trisection.

The Quadratrix of Hippias

Definition. In the unit square $OABC$, rotate a radial from OA to OC uniformly while a horizontal slides from OA to CB in equal time. Their intersection traces the *quadratrix*: at time t, angle $\theta = \frac{\pi}{2}t$ and height $y = t$, so $y = \frac{2}{\pi}\theta$ along the curve.

Trisecting any angle θ. Mark the quadratrix point P on the ray of angle θ (height $y = \frac{2}{\pi}\theta$). Trisect the segment to $y/3$ by line-and-compass, draw the horizontal at $y/3$, intersect the curve at P'. Then OP' has angle $\theta/3$.

Non-constructibility. As $\theta \to 0$ the curve meets OA at $D = (\frac{2}{\pi}, 0)$; $2/\pi$ is transcendental (Lindemann, 1882, used as a black box), so D is unreachable by line and compass.



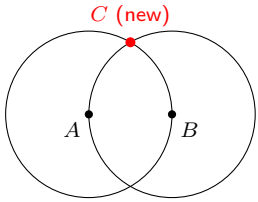
Constructed Points and Constructible Numbers

Constructed points are built recursively from $(0,0)$ and $(1,0)$:

- draw the *line* through two constructed points;
- draw the *circle* centered at a constructed point through a constructed point;
- a new point is an intersection of two such loci.

A real number α is **constructible** if some constructed segment has length $|\alpha|$; a point (x,y) is constructible iff x and y are.

Classical Euclidean moves are available: erect/drop perpendiculars, copy a length, draw parallels, bisect segments and angles. From the unit segment one locates every point with rational coordinates.



two unit circles centered at $A=(0,0)$ and $B=(1,0)$ meet at the new point $C=(\frac{1}{2},\frac{\sqrt{3}}{2})$ (Euclid I.1)

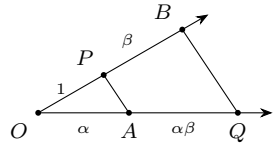
Constructible Numbers Form a Field

Theorem. If α, β are constructible, then so are $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, and α/β (for $\beta \neq 0$).

Proof.

- *Sum/difference:* lay the length $|\beta|$ off along the line carrying $|\alpha|$ with the compass.
- *Product:* on one ray from O lay $|OP| = 1$ then $|PB| = |\beta|$; on another lay $|OA| = |\alpha|$. The parallel to PA through B meets ray OA at Q, and by the intercept theorem $\frac{|OP|}{|PB|} = \frac{|OA|}{|AQ|}$, so $|AQ| = |\alpha\beta|$.
- *Quotient:* the analogous parallel construction yields $|\alpha/\beta|$. ■

Corollary. $F := \{\text{constructible reals}\}$ is a subfield of $\mathbb{R}$, and $\mathbb{Q} \subseteq F$.



product by similar triangles: $PA \parallel BQ$

Square Roots Are Constructible

Theorem. If $\alpha > 0$ is constructible, then $\sqrt{\alpha}$ is constructible.

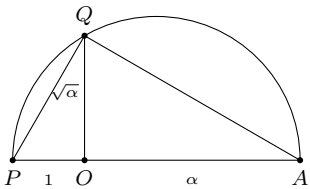
Proof (geometric mean).

(1) Mark P, O, A collinear with $|PO| = 1$ and $|OA| = \alpha$.

(2) Draw the semicircle on diameter PA; the perpendicular to PA at O meets it at Q.

(3) By Thales, $\angle PQA = 90^\circ$; so $\triangle OPQ \sim \triangle OQA$.

(4) $\dfrac{|OQ|}{|OP|} = \dfrac{|OA|}{|OQ|} \Rightarrow |OQ|^2 = 1 \cdot \alpha \Rightarrow |OQ| = \sqrt{\alpha}$. ■



Corollary. F is closed under $\sqrt{\ }$ of positive elements — the operation a compass adds beyond arithmetic.

Each Step Adjoins at Most One Square Root

Lemma. If every constructed point so far has coordinates in a subfield $H \subseteq \mathbb{R}$, then each new constructed point has coordinates in H or in a quadratic extension $H(\sqrt{d})$ with $d \in H$, $d \geq 0$.

Proof. The loci over H are:

- lines through two such points: $ax + by + c = 0$ with $a, b, c \in H$;
- circles centered at such a point through such a point: $x^2 + y^2 + dx + ey + f = 0$ with $d, e, f \in H$.

A new point is an intersection of two loci; three cases:

- **line ∩ line.** Two linear equations over H; the solution stays in H.
- **circle ∩ circle.** Subtracting the equations cancels $x^2 + y^2$, leaving a line over H (the *radical axis*); reduces to the line ∩ circle case.
- **line ∩ circle.** Substitution gives a quadratic over H, whose roots lie in $H(\sqrt{d})$ for some $d \in H$, $d \geq 0$.

In every case the coordinates lie in H or $H(\sqrt{d})$: degree over H is 1 or 2. ■

The Tower Characterization of F

Theorem. For $\alpha \in \mathbb{R}$, the following are equivalent.

1. α is constructible.
2. There is a tower $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ with $\alpha \in K_n$ and each $[K_i : K_{i-1}] = 2$ (so $K_i = K_{i-1}(\sqrt{d_i})$, $d_i \in K_{i-1}$, $d_i > 0$).
3. α is obtained from $\mathbb{Q}$ by finitely many field operations and square roots of positive numbers.

Proof.

- $(1) \Rightarrow (2)$: each new point adjoins one square root (previous Lemma); collect them into a tower whose top field K_n contains α.
- $(2) \Rightarrow (3)$: each step $K_{i-1}(\sqrt{d_i})$ is field operations plus one square root.
- $(3) \Rightarrow (1)$: F is a field containing $\mathbb{Q}$ and closed under positive square roots, so it contains every such expression. ∎

Part II: The Degree Criterion

Constructible Numbers Have 2-Power Degree

Corollary (Wantzel, 1837). If $\alpha \in \mathbb{R}$ is constructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^r$ for some integer $r \geq 0$.

Proof.

(1) By the tower characterization, $\alpha \in K_n$ for some tower with each $[K_i : K_{i-1}] = 2$.

(2) By the tower law, $[K_n : \mathbb{Q}] = \prod_{i=1}^{n} [K_i : K_{i-1}] = 2^n$.

(3) Since $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K_n$, the tower law gives

$$[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}].$$

(4) Hence $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divides 2^n and is a power of 2. ■

Use. To prove a length is *not* constructible, exhibit a number whose degree over $\mathbb{Q}$ is not a power of 2 — most cheaply, degree 3.

Necessary, Not Sufficient

The converse fails. The degree criterion is necessary but not sufficient.

Counterexample. Let α be a root of an irreducible quartic $f \in \mathbb{Q}[x]$ whose splitting field has Galois group S_4. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ is a power of 2, yet α is *not* reachable by a tower of quadratic extensions ($|S_4| = 24$, not a 2-power).

Definition (Galois closure). The *Galois closure* of an algebraic extension E/F is the smallest field extension of F containing E that is Galois over F. Over $\mathbb{Q}$ (every algebraic extension is separable in characteristic 0), the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$ equals the splitting field of $\mathrm{irr}(\alpha, \mathbb{Q})$.

Sharp condition (Galois criterion). α is constructible iff its Galois closure L satisfies

$$[L : \mathbb{Q}] = 2^m, \qquad \text{equivalently,} \qquad \mathrm{Gal}(L/\mathbb{Q}) \text{ is a 2-group.}$$

For the three classical problems the necessary direction (degree criterion) already suffices, so we settle them first.

Part III: The Three Impossibility Proofs

Doubling the Cube Is Impossible

Theorem. One cannot construct, with straightedge and compass, the edge of a cube of twice the volume of a given cube.

Proof.

(1) Normalize the given edge to 1; the target edge has length $\sqrt[3]{2}$.

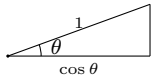
(2) $x^3 - 2$ is irreducible over $\mathbb{Q}$ (Eisenstein at $p = 2$).

(3) Hence $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

(4) 3 is not a power of 2, so the degree criterion gives $\sqrt[3]{2} \notin F$. ■

The Triple-Angle Cubic for $\cos 20^\circ$

Lemma (angle $\leftrightarrow$ cosine). An angle θ is constructible iff a segment of length $|\cos\theta|$ is constructible. *(Right triangle with hypotenuse 1: adjacent leg has length $|\cos\theta|$.)*



Triple-angle identity. From $\cos 3\theta = \cos(2\theta + \theta)$ and the addition formulas,

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

Specializing to $\theta = 20^\circ$. Then $\cos 3\theta = \cos 60^\circ = \frac{1}{2}$, so with $\alpha = \cos 20^\circ$,

$$4\alpha^3 - 3\alpha = \tfrac{1}{2}, \qquad \text{i.e.} \qquad 8\alpha^3 - 6\alpha - 1 = 0.$$

Trisecting the Angle Is Impossible

Theorem. The angle 60° cannot be trisected by straightedge and compass.

Proof.

(1) 60° is constructible (equilateral triangle).

(2) Trisecting 60° means constructing $\alpha = \cos 20^\circ$, a root of $f(x) = 8x^3 - 6x - 1$.

(3) Substitute $x = y + \frac{1}{2}$: $f\big(y + \frac{1}{2}\big) = 8y^3 + 12y^2 - 3$.

(4) Eisenstein at $p = 3$: $3 \nmid 8$, $3 \mid 12$, $3 \mid -3$, $9 \nmid -3$. So $f(y + \frac{1}{2})$ is irreducible over $\mathbb{Q}$, hence so is $f(x)$.

(5) Hence $[\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}] = 3$.

(6) 3 is not a power of 2, so $\cos 20^\circ$ is not constructible, and 60° is not trisectable. ■

Remark. Some angles do trisect (e.g. $90^\circ \to 30^\circ$); the theorem is that no single straightedge-and-compass method trisects *every* angle.

Squaring the Circle Is Impossible

Theorem. One cannot construct a square equal in area to a given circle.

Cited input (Lindemann, 1882). π is *transcendental* over $\mathbb{Q}$: no nonzero polynomial in $\mathbb{Q}[x]$ vanishes at π. (Proof beyond this course; used as a black box.)

Proof.

(1) For the unit circle (area π) the equal-area square has side $\sqrt{\pi}$.

(2) If $\sqrt{\pi}$ were constructible, so would $\pi = (\sqrt{\pi})^2$.

(3) A constructible number is algebraic of 2-power degree over $\mathbb{Q}$ (degree criterion).

(4) But π is transcendental, hence not algebraic. Contradiction. ∎

Ferdinand von Lindemann (1852–1939): proved π transcendental in 1882.

Part IV: Regular Polygons and the Galois Criterion

Constructibility in the Plane

Definition. Identify the plane with $\mathbb{C}$. A complex number $z = a + bi$ is **constructible** iff $a, b \in F$. The constructible complex numbers form a subfield $\mathbb{K} \subseteq \mathbb{C}$ containing $\mathbb{Q}$.

Proposition. $\mathbb{K}$ is closed under square roots.
Proof. If $z = \rho\, e^{i\psi} \in \mathbb{K}$, construct $\sqrt{\rho}$ (geometric mean) and bisect the angle ψ; this gives $\sqrt{\rho}\, e^{i\psi/2} \in \mathbb{K}$. $\square$

Proposition (Complex tower characterization). For $z \in \mathbb{C}$, $z \in \mathbb{K}$ iff z lies in a tower $\mathbb{Q} = K_0 \subseteq \cdots \subseteq K_n \subseteq \mathbb{C}$ with each $[K_i : K_{i-1}] = 2$.
Proof. ($\Leftarrow$) each step adjoins a $\sqrt{\ }$, which $\mathbb{K}$ contains. ($\Rightarrow$) $z = a + bi$ with $a, b \in F$ sits in a real quadratic tower; one more quadratic step adjoins $i = \sqrt{-1}$. $\square$

The Regular n-gon Reduces to $\cos(2\pi/n)$

Inscribe the regular n-gon in the unit circle with one vertex at 1. Its vertices are the powers ζ_n^k of

$$\zeta_n = e^{2\pi i/n} = \cos\tfrac{2\pi}{n} + i\sin\tfrac{2\pi}{n}.$$

Therefore:

- the n-gon is constructible $\iff$ ζ_n is constructible;
- ζ_n is constructible $\iff$ $\cos(2\pi/n)$ is constructible, since then $\sin(2\pi/n) = \sqrt{1-\cos^2(2\pi/n)}$ is constructible too.

So the geometric question becomes: *for which n is $\cos(2\pi/n)$ constructible?* The Galois criterion answers it.

The Galois Criterion for Constructibility

Theorem. Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$, and let L be the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$ (equivalently, the splitting field of $\mathrm{irr}(\alpha, \mathbb{Q})$). Then

$$\alpha \text{ constructible} \iff [L : \mathbb{Q}] = 2^m \iff \mathrm{Gal}(L/\mathbb{Q}) \text{ is a 2-group.}$$

Proof of $\Leftarrow$ (sufficiency).

(1) Let $G = \mathrm{Gal}(L/\mathbb{Q})$ have order 2^m.

(2) As a finite p-group, G is nilpotent; hence it admits a chief series with cyclic factors of order 2:

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_m = \{1\}, \qquad [G_i : G_{i+1}] = 2.$$

(3) Galois correspondence ($G_i \leftrightarrow F_i$) gives a tower of fields

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = L, \qquad [F_{i+1} : F_i] = 2.$$

(4) Each step is a quadratic extension, so $\alpha \in L = F_m$ lies in a quadratic tower and is constructible. ■

The Galois Criterion: Necessity

Proof of $\Rightarrow$.

(1) If α is constructible, then $\alpha \in K_n$ for some quadratic tower

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n, \qquad [K_i : K_{i-1}] = 2.$$

(2) Every quadratic extension is normal (the conjugate $-\sqrt{d}$ already lies in $K_{i-1}(\sqrt{d})$), and char $\mathbb{Q} = 0$ gives separability, so each step is Galois.

(3) Let $\widetilde{L}$ be the Galois closure of $K_n/\mathbb{Q}$. Build $\widetilde{L}$ by adjoining, one at a time, the $\mathbb{Q}$-conjugates of $\sqrt{d_1}, \ldots, \sqrt{d_n}$; each conjugate is a square root over the current field, so each adjunction has degree 1 or 2. Hence $[\widetilde{L} : \mathbb{Q}] = 2^N$.

(4) The theorem's L (closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$) sits inside $\widetilde{L}$, so $[L : \mathbb{Q}]$ divides 2^N and is itself a power of 2. Therefore $\mathrm{Gal}(L/\mathbb{Q})$ is a 2-group. ■

Reading. The *closure* must be a 2-group — not merely $\mathbb{Q}(\alpha)$ of 2-power degree — which is why the degree criterion is necessary but not sufficient.

The Cyclotomic Polynomial Φ_n

Definition. Set $\zeta_n = e^{2\pi i/n}$. A *primitive* n-th root of unity is ζ_n^k with $\gcd(k,n)=1$ ($\varphi(n)$ of them). The n-th cyclotomic polynomial is

$$\Phi_n(x) := \prod_{\substack{1\le k\le n\\ \gcd(k,n)=1}} (x-\zeta_n^k) \in \mathbb{C}[x], \qquad \deg \Phi_n = \varphi(n).$$

Proposition (Product formula). For every $n \ge 1$,

$$x^n - 1 \;=\; \prod_{d\mid n} \Phi_d(x).$$

Proof. Every n-th root of unity has a unique order d dividing n, and is then a primitive d-th root. Grouping the roots of x^n-1 by their order yields the factorization on the right. $\square$

Corollary. Φ_n is monic with integer coefficients ($\Phi_n \in \mathbb{Z}[x]$).
Proof. Induction on n via $\Phi_n = (x^n-1)\big/\prod_{d\mid n,\, d<n} \Phi_d$: the right side is a quotient of monic polynomials in $\mathbb{Z}[x]$, so monic in $\mathbb{Z}[x]$. $\square$

$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois

Proposition. The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois.

Proof.

- Every n-th root of unity is a power of ζ_n, so $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1 \in \mathbb{Q}[x]$.
- $x^n - 1$ is separable over $\mathbb{Q}$: $\gcd(x^n - 1,\, nx^{n-1}) = 1$ in $\mathbb{Q}[x]$ (the only root of nx^{n-1} is 0, which is not a root of $x^n - 1$).
- A splitting field of a separable polynomial is Galois.

□

Φ_n for Small n and Reduction Identities

Small cases. The recursion $x^n - 1 = \prod_{d|n} \Phi_d(x)$ computes Φ_n from smaller Φ_d by polynomial division:

n	$\Phi_n(x)$
1	$x - 1$
2	$x + 1$
3	$x^2 + x + 1$
4	$x^2 + 1$
5	$x^4 + x^3 + x^2 + x + 1$
6	$x^2 - x + 1$
7	$x^6 + x^5 + \cdots + x + 1$
8	$x^4 + 1$
9	$x^6 + x^3 + 1$
10	$x^4 - x^3 + x^2 - x + 1$
12	$x^4 - x^2 + 1$

Identities (each by matching primitive-root sets).

- **Prime p.**

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

- **Prime power.** $\Phi_{p^k}(x) = \Phi_p\left(x^{p^{k-1}}\right)$. E.g. $\Phi_8(x) = \Phi_2(x^4) = x^4 + 1$.
- **Doubling.** For odd $n \geq 3$, $\Phi_{2n}(x) = \Phi_n(-x)$ (uses $-\zeta$ primitive $2n$-th iff ζ primitive n-th). E.g. $\Phi_6(x) = x^2 - x + 1$.

Coefficients stay in $\{-1, 0, 1\}$ for small n; first exception Φ_{105}.

Irreducibility of Φ_p (Eisenstein)

Theorem. For p prime, Φ_p is irreducible over $\mathbb{Q}$.

Proof.

(1) $\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$

(2) Substitute $x \mapsto x + 1$:

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-1}.$$

(3) Check Eisenstein conditions at p for $\Phi_p(x+1)$:

- Leading coefficient 1: not divisible by p.
- Each interior coefficient $\binom{p}{k}$ $(1 \le k \le p-1)$: divisible by p (the numerator carries a factor p that $k!(p-k)!$ cannot cancel).
- Constant term $\binom{p}{p-1} = p$: divisible by p but not by p^2.

(4) By Eisenstein, $\Phi_p(x+1)$ is irreducible. Since $x \mapsto x + 1$ is an automorphism of $\mathbb{Q}[x]$, so is Φ_p. ■

Reach. Same trick handles Φ_{p^k}. For n with two or more distinct prime factors, no substitution gives Eisenstein — the Dedekind-style mod-p argument takes over.

The Cyclotomic Frobenius Lemma

Lemma (Dedekind, 1857). Suppose $\Phi_n = fg$ in $\mathbb{Z}[x]$ with f, g monic. Let p be a prime with $p \nmid n$, and let ζ be a root of f in $\overline{\mathbb{Q}}$. Then ζ^p is also a root of f.

Proof.

Assume the contrary. If ζ^p is not a root of f, it must be a root of g (since ζ^p is a root of $\Phi_n = fg$). Then ζ is a root of $g(x^p)$, so $f(x) \mid g(x^p)$ in $\mathbb{Z}[x]$.

Reduce mod p. The Frobenius identity in characteristic p gives $\bar{g}(x^p) = \bar{g}(x)^p$; hence $\bar{f}(x) \mid \bar{g}(x)^p$ in $\mathbb{F}_p[x]$. So $\bar{f}$ and $\bar{g}$ share an irreducible factor, and $\bar{\Phi}_n = \bar{f}\,\bar{g}$ has a multiple root in $\overline{\mathbb{F}_p}$.

Contradiction. $\Phi_n \mid x^n - 1$, and $x^n - 1$ is separable mod p when $p \nmid n$ (its derivative nx^{n-1} is coprime to it). So $\bar{\Phi}_n$ has no multiple roots — contradiction. ∎

Irreducibility of Φ_n

Theorem (Gauss, 1801). Φ_n is irreducible over $\mathbb{Q}$.

Proof (Dedekind, 1857).

Setup. Let f be the minimal polynomial of ζ_n over $\mathbb{Q}$ (monic in $\mathbb{Q}[x]$). Since ζ_n is a root of $x^n - 1 \in \mathbb{Z}[x]$, f divides $x^n - 1$ in $\mathbb{Q}[x]$. By Gauss's lemma (*a monic polynomial in* $\mathbb{Q}[x]$ *that divides a monic polynomial in* $\mathbb{Z}[x]$ *already lies in* $\mathbb{Z}[x]$), $f \in \mathbb{Z}[x]$. Write $\Phi_n = fg$ in $\mathbb{Z}[x]$.

Iteration. Any primitive n-th root has the form ζ_n^k with $\gcd(k, n) = 1$. Factor $k = p_1 \cdots p_r$ (each $p_i \nmid n$), and apply the Cyclotomic Frobenius Lemma successively:

$$\zeta_n \;\mapsto\; \zeta_n^{p_1} \;\mapsto\; \zeta_n^{p_1 p_2} \;\mapsto\; \cdots \;\mapsto\; \zeta_n^{k},$$

each step taking a root of f to a root of f.

Conclusion. Every primitive root is a root of f, so $\Phi_n \mid f$; combined with $f \mid \Phi_n$ and both monic, $f = \Phi_n$. ∎

Cyclotomic Galois Group: The Map Ψ

Theorem. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Order count. Φ_n is the minimal polynomial of ζ_n over $\mathbb{Q}$, so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \varphi(n)$. Since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois,

$$|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

Define the map. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Since σ fixes $\mathbb{Q}$ and $\Phi_n \in \mathbb{Q}[x]$, σ permutes the roots of Φ_n in $\mathbb{Q}(\zeta_n)$. The roots of Φ_n are exactly the primitive n-th roots $\{\zeta_n^a : \gcd(a, n) = 1\}$. So $\sigma(\zeta_n) = \zeta_n^a$ for some integer a with $\gcd(a, n) = 1$, unique modulo n. Set

$$\Psi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \qquad \sigma \mapsto a \bmod n \ \text{ where } \sigma(\zeta_n) = \zeta_n^a.$$

Cyclotomic Galois Group: Ψ is an Isomorphism

(a) Homomorphism. For $\sigma, \tau \in \mathrm{Gal}$ with $\sigma(\zeta_n) = \zeta_n^a$ and $\tau(\zeta_n) = \zeta_n^b$,

$$(\sigma \circ \tau)(\zeta_n) = \sigma(\zeta_n^b) = (\sigma(\zeta_n))^b = \zeta_n^{ab},$$

so $\Psi(\sigma\tau) = ab \bmod n = \Psi(\sigma)\Psi(\tau)$.

(b) Injective. If $\Psi(\sigma) = 1 \bmod n$, then $\sigma(\zeta_n) = \zeta_n$. Since ζ_n generates $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ and σ fixes $\mathbb{Q}$, $\sigma = \mathrm{id}$.

(c) Bijective. Both groups have order $\varphi(n)$, and an injective homomorphism between finite groups of the same order is bijective. ■

Notation. Write $\sigma_a := \Psi^{-1}(a \bmod n)$, the unique automorphism with $\sigma_a(\zeta_n) = \zeta_n^a$. Under Ψ, composition of automorphisms becomes multiplication mod n: $\sigma_a\sigma_b = \sigma_{ab}$.

Cyclotomic Examples and Constructibility

Small cases.

- $n = p$ prime: $(\mathbb{Z}/p)^\times$ is cyclic of order $p - 1$.
- $n = 5$: $(\mathbb{Z}/5)^\times = \{1, 2, 3, 4\} \cong \mathbb{Z}/4$ (generated by 2).
- $n = 8$: $(\mathbb{Z}/8)^\times = \{1, 3, 5, 7\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ (Klein four-group; every element squares to 1).
- $n = 12$: $(\mathbb{Z}/12)^\times = \{1, 5, 7, 11\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

Constructibility of ζ_n. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois (its own Galois closure) and has degree $\varphi(n)$. By the Galois criterion (ζ_n constructible iff its Galois closure has 2-power degree),

$$\zeta_n \text{ constructible} \iff \varphi(n) \text{ is a power of } 2.$$

Fermat Primes

Definition. A *Fermat number* is $F_t = 2^{2^t} + 1$; a *Fermat prime* is a Fermat number that is prime.

Known Fermat primes.

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537.$$

Fermat's conjecture (1640). Fermat believed every F_t is prime.

Euler's refutation (1732).

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417.$$

Status today. $F_5, \ldots, F_{32}$ (and many beyond) are all known composite. No further Fermat prime has ever been found; whether there are infinitely many—or only these five—remains open.

Pierre de Fermat (1607–1665). Conjectured all F_t prime; Euler found $641 \mid F_5$.

The Gauss–Wantzel Theorem

Theorem. The regular n-gon ($n \geq 3$) is constructible if and only if

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

with $k \geq 0$ and the p_i distinct Fermat primes.

Proof.

(1) n-gon constructible $\iff$ ζ_n constructible $\iff$ $\varphi(n)$ is a 2-power.

(2) Write $n = 2^{a_0} \prod_i p_i^{a_i}$ with p_i distinct odd primes. Then

$$\varphi(n) = \varphi(2^{a_0}) \prod_i p_i^{a_i - 1}(p_i - 1).$$

(3) $\varphi(2^{a_0})$ is always a 2-power, so $\varphi(n)$ is a 2-power iff every $a_i = 1$ and every $p_i - 1$ is a 2-power.

(4) An odd prime p with $p - 1 = 2^e$ is a Fermat prime $p = 2^{2^t} + 1$ (Fermat-prime characterization, proved next). ■

$p - 1 = 2^e$ Forces $p = 2^{2^t} + 1$

Claim. If p is an odd prime and $p - 1 = 2^e$, then $e = 2^t$ for some $t \geq 0$ — i.e. $p = 2^{2^t} + 1$.

Proof.

(1) Suppose, for contradiction, that e has an odd factor $v \geq 3$. Write $e = uv$ with $u \geq 1$ (so $u < e$).

(2) For any odd v, $y^v + 1$ has root $y = -1$, giving

$$y^v + 1 = (y + 1)\big(y^{v-1} - y^{v-2} + \cdots - y + 1\big).$$

(3) Set $y = 2^u$:

$$2^e + 1 = (2^u)^v + 1 = (2^u + 1) \cdot Q, \qquad Q \in \mathbb{Z}_{>0}.$$

(4) So $2^u + 1 \mid p = 2^e + 1$. And $u \geq 1 \Rightarrow 2^u + 1 \geq 3$; $u < e \Rightarrow 2^u + 1 < 2^e + 1 = p$. So $2^u + 1$ is a *proper* divisor of p — contradicting primality.

(5) Hence e has no odd factor > 1: $e = 2^t$. ■

Gauss and the Regular 17-gon

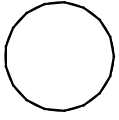
In 1796, aged 19, Gauss found the regular 17-**gon** constructible — $\varphi(17) = 16 = 2^4$ — and opened his *Disquisitiones Arithmeticae* (1801) with it. He gave the explicit value

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

$$+\tfrac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}},$$

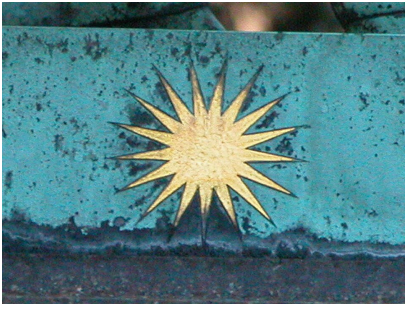
a tower of nested square roots — exactly a quadratic tower. Gauss stated the full classification and proved the constructible half.

C. F. Gauss (1777–1855).



Gauss's Tomb and Memorial

Gauss's grave, Albani-Friedhof, Göttingen.



17-pointed star on the Gauss-Denkmal (Braunschweig; statue 1880).

Gauss reportedly asked for a regular 17-gon on his tombstone; the mason refused, saying it would look like a circle. The 17-pointed star on the Brunswick memorial stands in.

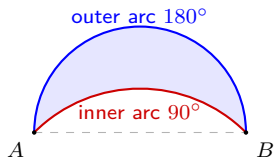
The Five Squarable Lunes

A *lune* is a crescent bounded by two circular arcs sharing endpoints. Hippocrates of Chios (c. 440 BC) squared certain lunes by straightedge and compass — the first exact squaring of any curvilinear region.

Squarable arc-ratios.

- Hippocrates: $2{:}1,\ 3{:}1,\ 3{:}2$.
- Wallenius (1766): $5{:}1,\ 5{:}3$.
- Tschebotarëw (1934) – Dorodnov (1947): these five are the *only* squarable lunes with rational arc-ratio.

The circle has only one arc, so it is no lune. Lindemann (1882) settles it separately.



Hippocrates' $2{:}1$ lune (shaded).

Mohr–Mascheroni and Poncelet–Steiner

Two equivalence theorems. Neither enlarges the constructible set, but each shows one of the two classical instruments is redundant.

Mohr (1672) – Mascheroni (1797). Every straightedge-and-compass construction can be carried out by the *compass alone*—if a "line through two given points" is identified with the pair of points (no physical line drawn). Mascheroni published this in *La geometria del compasso* (1797); Georg Mohr's earlier *Euclides Danicus* (1672) was forgotten until 1928.

Poncelet (1822) – Steiner (1833). Every straightedge-and-compass construction can be carried out by the *straightedge alone*, given one auxiliary circle in the plane with its centre marked. Conjectured by Poncelet, proved by Jakob Steiner. The marked centre is essential: Steiner also showed an unmarked circle is not enough.

Reading. The genuinely new operation in Euclidean construction is the compass; the straightedge is dispensable in one direction, and almost dispensable in the other.

Pierre Wantzel

Pierre Laurent Wantzel (1814–1848). Parisian child prodigy; entered the École Polytechnique in 1832, then the École des Ponts et Chaussées; taught mathematics and mechanics at several Paris schools.

The 1837 paper. *Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas* (*Journal de Liouville*, vol. 2) sets down the degree obstruction $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^r$ that drives this lecture — and uses it to settle doubling the cube, trisecting general angles, and the necessity half of Gauss's n-gon classification.

Aftermath. He died at 33, exhausted by overwork sustained on coffee and opium (Saint-Venant obituary, *Nouvelles Annales de Mathématiques*, 1848). The 1837 paper went uncelebrated in his lifetime.

How Lindemann Proved π Transcendental

Building on Hermite's 1873 proof that e is transcendental, Lindemann proved:

Lindemann's Theorem (1882). *If $\alpha_1, \ldots, \alpha_n$ are distinct algebraic numbers, then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are linearly independent over $\overline{\mathbb{Q}}$.*

Reduction to π. If π were algebraic, so would $i\pi$ ($\overline{\mathbb{Q}}$ is a field). The theorem applied to the distinct algebraic numbers 0 and $i\pi$ says $e^0 = 1$ and $e^{i\pi} = -1$ are linearly independent. But $1 \cdot 1 + 1 \cdot (-1) = 0$. Contradiction.

Inside the theorem. Build an auxiliary polynomial, integrate e^{α} against it, and force a nonzero integer below 1. Seed of modern transcendence theory (Lindemann–Weierstrass 1885, Gelfond–Schneider 1934, Baker 1966).

Ferdinand von Lindemann (1852–1939). 1882 paper *Über die Zahl π* (*Math. Ann.*) settles squaring the circle.