Cheat Sheet due Today.

Today: Gauss-Wantzel + Beyond.

Last Time: If $f(x) \in \mathbb{Q}[x]$ has degree 3 and no root in $\mathbb{Q}$, then it has no root in $\mathbb{Q}_{sqrt}$.

Corollaries:

- Algebraic: The numbers $\sqrt[3]{2}$, $\cos\left(\frac{2\pi}{9}\right)$, $\cos\left(\frac{2\pi}{7}\right)$ cannot be expressed in terms of $\mathbb{Q}$ and square roots.
- Geometric: Straight edge & compass constructions "double cube" "trisect angle" "regular heptagon" are impossible.

How does this generalize to polynomials of degree ≥ 4?

Example: We know regular n-gon $\iff$ $3 \leq n \leq 10$ except $n = 7$.

What about $n \geq 11$?

Equivalently, for which n do we have $\cos\left(\frac{2\pi}{n}\right) \in \mathbb{Q}_{sqrt}$?

i.e., how complicated is the number $\cos\left(\frac{2\pi}{n}\right)$? Can it be expressed in terms of $\sqrt{\ }$? Or do we need $\sqrt[3]{\ }$?

etc.

This problem was solved by Gauss (age of 23) in Chapter 7 of his book "Disquisitiones Arithmeticae."

I will describe the theorem in modern language.

Let $\alpha \in \mathbb{R}$ (or $\in \mathbb{C}$)

- If $f(\alpha) \neq 0$ for $^{\text{all}}$ $f(x) \in \mathbb{Q}[x]$, we say α is "transcendental / $\mathbb{Q}$"
- If $f(\alpha) = 0$ for some $f(x) \in \mathbb{Q}[x]$ then we say α is "algebraic / $\mathbb{Q}$",

in which case there exists a unique monic (Leading coeff = 1) polynomial $\in \mathbb{Q}[x]$ of minimal degree having α as a root:

$$p_\alpha(x) \in \mathbb{Q}[x]$$

the "minimal polynomial of $\alpha/\mathbb{Q}$"

- Furthermore, this $p_\alpha(x)$ is <u>prime</u> $/\mathbb{Q}$ and we have a generalization of Descartes' Theorem:

Given $f(x) \in \mathbb{Q}[x]$,

$f(\alpha) = 0 \iff f(x) = p_\alpha(x)g(x)$ for some $g(x) \in \mathbb{Q}[x]$ //

Examples:

- If $\alpha \in \mathbb{Q}$ then $p_\alpha(x) = x - \alpha$.
- $p_{\sqrt{-1}}(x) = x^2 + 1$.
- $p_{\sqrt{2}}(x) = x^2 - 2$.

• Our work last time amounts to the statements

$$p_{\sqrt[3]{2}}(x) = x^3 - 2,$$

$$p_{2\cos(\frac{2\pi}{7})}(x) = x^3 - 3x + 1,$$

$$p_{2\cos(\frac{2\pi}{7})}(x) = x^3 + x^2 - 2x - 1.$$

[By showing these have no roots in $\mathbb{Q}$, we showed they are prime/$\mathbb{Q}$ because 3 is a small number.]

For higher degrees, it is not so easy to show that a polynomial is prime/$\mathbb{Q}$.

Theorem (Gauss 1808, Wantzel 1837):
Let α be algebraic/$\mathbb{Q}$. Then

$$\alpha \in \mathbb{Q}_{sqrt} \iff \deg(p_\alpha) = \text{power of } 2.$$

Furthermore, the min. poly. of $\cos(\frac{2\pi}{n})$ has degree $\phi(n)/2$, where

$$\phi(n) = \#\{1 \le k \le n : \gcd(k,n) = 1\}.$$

It follows that

n-gon is c'ble $\iff \cos\left(\frac{2\pi}{n}\right) \in \mathbb{Q}_{sqrt}$

$\iff \phi(n)/2 =$ power of 2

$\iff \phi(n) =$ power of 2.

[Remark: $\iff$ $n =$ power of 2 times product of distinct "Fermat primes."]

Proof? The polynomial $p_{\cos(\frac{2\pi}{n})}(x)$ is complicated to describe, but is closely related to following fact:

$$\boxed{p_{e^{2\pi i/n}}(x) = \Phi_n(x)}$$

Indeed, you showed $\Phi_n(x) \in \mathbb{Q}[x]$

(and Leading coeff. $= 1$). However, it is very difficult to prove that $\Phi_n(x)$ is prime / $\mathbb{Q}$.

[Even Gauss only proved this when n is prime.]

Next: Observe $\deg(\Phi_n(x)) = \phi(n)$.

If $\deg(\Phi_n(x)) = \phi(n) =$ power of 2, Gauss showed that $\omega = e^{2\pi i/n} \in \mathbb{Q}_{sqrt}$.

(hence also $\cos\left(\frac{2\pi}{n}\right) \in \mathbb{Q}_{sqrt}$).

(That is, it was easier to prove c'bility of complex number ω, then obtain c'bility of real number $\cos\left(\frac{2\pi}{n}\right)$.]

In fact, Gauss stated a more general theorem: Let $\omega = e^{2\pi i/n}$.

Suppose $\phi(n) = m_1 m_2 \cdots m_k$ $(m_i \geq 2)$.

Then the exists a chain of subfields

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_k = \mathbb{Q}(\omega)$$

with the property that:

every $\alpha \in \mathbb{F}_i$ is a root of some $f_i(x) \in \mathbb{F}_{i-1}$ of degree m_i.

In particular, if $\phi(n) = 2^k$ then we can obtain ω from $\mathbb{Q}$ by solving a sequence of quadratic equations, hence $\omega \in \mathbb{Q}_{sqrt}$, and the same applies to $\omega + \omega^{-1} = 2\cos\left(\frac{2\pi}{n}\right)$.

Gauss only proved this theorem for the case $n = p$ prime. Even then, the proof involved a wealth of new ideas, and was not fully understood until the 1880s.

Here's a sketch in modern language:

- $\exists$ integer r such that

$$\{\omega, \omega^2, \ldots, \omega^{p-1}\} = \{\omega^r, \omega^{(r^2)}, \ldots, \omega^{(r^{p-1})}\}$$

[This r is called a "primitive root".]

- $\exists$ "field automorphism"

$$\varphi : \mathbb{F}_q(\omega) \longrightarrow \mathbb{F}_q(\omega)$$
$$\omega \longmapsto \omega^r$$

[Automorphism means φ is bijection, $\varphi(\alpha+\beta) = \varphi(\alpha) + \varphi(\beta)$, $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.]

- φ^{p-1} = identity function.

- For $d \mid p-1$, define the set

$$\mathbb{F}_d = \{\alpha \in \mathbb{F}_q(\omega) : \varphi^d(\alpha) = \alpha\}.$$

This set is a field and for $d \mid e \mid p-1$ we have $\mathbb{F}_d \subseteq \mathbb{F}_e$.

- $\mathbb{F}_{p-1} = \{\alpha : id(\alpha) = \alpha\} = \mathbb{F}_q(\omega)$
$\mathbb{F}_1 = \{\alpha : \varphi(\alpha) = \alpha\} = \mathbb{F}_q$

- For $d \mid e \mid p-1$, every element α of the field $\mathbb{F}_e$ is a root of some polynomial $\in \mathbb{F}_d[x]$ of degree e/d.

In fact, Gauss showed that the polynomial

$$(x-\alpha)(x-\varphi^{d}(\alpha))(x-\varphi^{2d}(\alpha))\cdots(x-\varphi^{d(\frac{e}{f}-1)}(\alpha))$$

has coefficients in $\mathbb{F}_d$.

QED.

Corollary: Since $\phi(17) = 16 = 2^4$, we can express $e^{2\pi i/17}$ and hence $\cos(\frac{2\pi}{17})$ in terms of square roots.

[We could obtain an explict formula from the above algorithm, but it would be to wide to fit on the page.]

Gauss discovered this result at the age of 19 and published his first paper detailing a construction of the regular 17-gon.

Thus, Chapter 7 of the Disquisitiones completely solved the cyclotomic equation

$$x^n - 1 = 0$$
$$\Phi_n(x) = 0.$$

What about other kinds of equations?

Évariste Galois is one of the most colorful characters in the history of mathematics. [I linked to a short biography on the course webpage.]

Galois died at the age of 20, but in his short life he discovered how to apply Gauss' ideas to any algebraic number $\alpha \in \mathbb{C}$:

- Consider the "group" of field automorphisms

$$\varphi : \mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}(\alpha)$$

- Use automorphisms to understand chains of subfields

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_k = \mathbb{Q}(\tau)$$

Of course, I have expressed Gauss' & Galois' insights in modern language. In fact, the modern language of "groups, rings, fields" developed over 100 years 1830 – 1930 through the attempt to understand what they had done.

This involved the creation of a completely new subject:

"Abstract Algebra"

[A full treatment of "Galois Theory" would require 2 more semesters. See my notes (soon a book) from MTH 561/562.]