Lecture 8.2

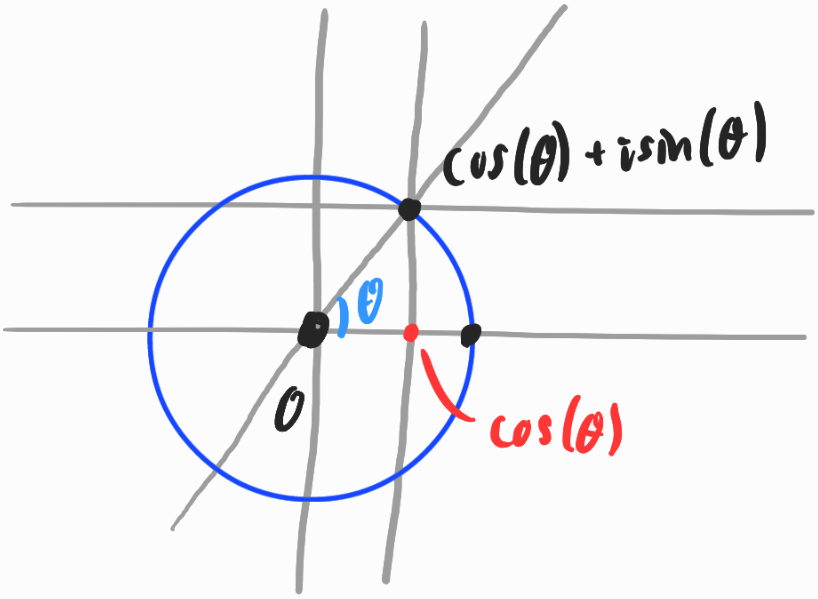
Last time:

- The set C of constructible numbers is a subfield of $\mathbb{C}$.
- For any $\alpha \in C$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ for some $n \geq 0$.
- It is impossible to square a circle and double a cube.

Corollary It is impossible to trisect an angle.

Pf: Suppose θ has been constructed.

Then $\cos(\theta)$ is also constructible:



This actually allows to trisect some angles, e.g. $\pi/2$, but not all angles.

Let $\theta = \pi/9$, which would trisect the constructible angle $\pi/3$.

Then $2\cos(\theta) = e^{\pi i/9} + e^{-\pi i/9}$ which satisfies

$$(2\cos(\theta))^3 = \left(e^{\pi i/9} + e^{-\pi i/9}\right)^3$$

$$= e^{\pi i/3} + 3e^{\pi i/9} + 3e^{-\pi i/9} + e^{-\pi i/3}$$

$$= 2\cos(\pi/3) + 3(2\cos(\theta)).$$

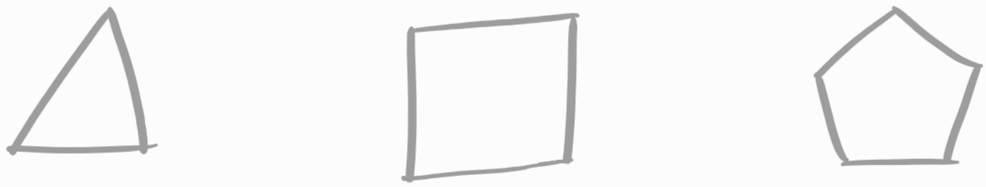
This shows that $\alpha = \cos(\theta)$ is a root of $8x^3 - 6x - 1$, which is irreducible (check it!) and therefore

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3.$$

Hence $\cos(\theta)$ is not constructible, so θ is not constructible. $\square$

Exercise 1: Prove that $2\pi/3$ cannot be trisected. Can you characterize those angles which can be trisected?

Def For $n \geq 3$, a **regular n-gon** is a polygon with n sides of equal length and n equal interior angles.



equilateral triangle | square | regular pentagon

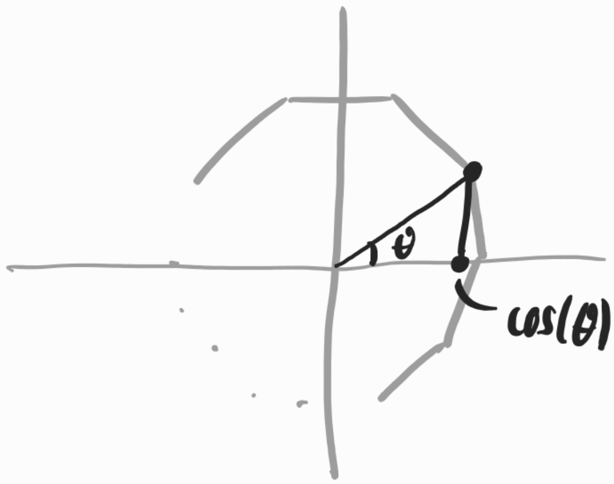
Q: For which n is a regular n-gon constructible?

Theorem If n is prime and a regular

Theorem If p is prime and a regular p-gon is constructible, then p is a Fermat prime, i.e. $p = 2^{2^k}+1$ for some $k \geq 0$.

Pf: If a regular p-gon is constructible, so is its interior angle $\theta = \frac{2\pi}{p}$.

As we showed above, this implies $\alpha \in C$ where $\alpha = \cos(\theta)$.



it will make sense below

Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^{n-1}$ for some $n \geq 1$.

Notice that $\zeta_p = e^{2\pi i/p} = e^{i\theta}$ is a root of

$$x^2 - 2\alpha x + 1 = 0.$$

This implies $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = 2^n$ by the tower law.

On the other hand, ζ_p is a root of $x^p - 1$ which factors as

$$x^p - 1 = (x-1)(x^{p-1} + \dots + x^2 + x + 1).$$

You will show on HW 7 that $x^{p-1} + \dots + x + 1$ is irreducible over $\mathbb{Q}$, meaning it's the minimal polynomial of ζ_p over $\mathbb{Q}$.

So $2^n = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, or

$$p = 2^n + 1.$$

Finally, the only primes of the form $2^n + 1$ have $n = 2^k$ for some $k \geq 0$. $\square$

Exercise 2: Prove that if $p = 2^n + 1$ is prime, then $n = 2^k$ for some $k \geq 0$.

Remark: There are only 5 known Fermat primes, for $k = 0, 1, 2, 3$ and 4. For $k = 5$, Euler showed that $2^{32}+1$ is composite, and so far, all $2^{2^k}+1$ have been shown to be composite for $5 \leq k \leq 32$, with many more sporadic examples also known.

More generally:

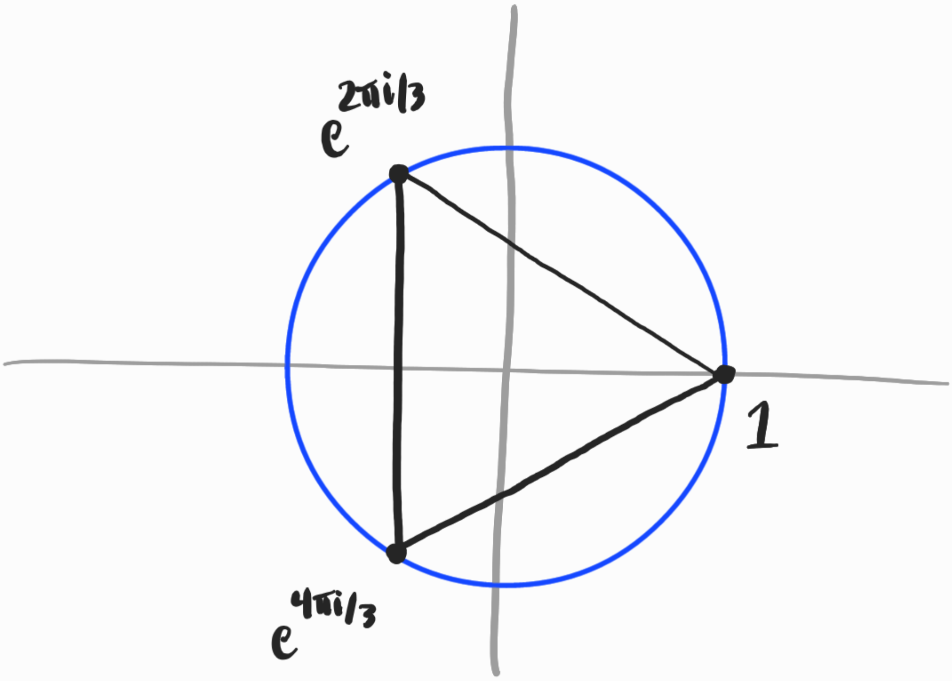
$\boxed{\text{Theorem (Gauss)}}$ For $n \geq 3$, a regular n-gon is constructible if and only if

$$n = 2^m p_1 \cdots p_r$$

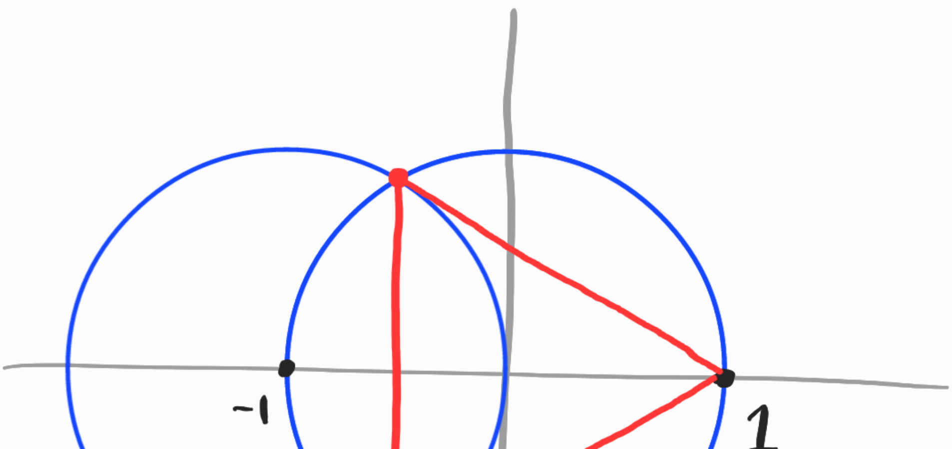
where $p_1, \dots, p_r$ are distinct Fermat primes.

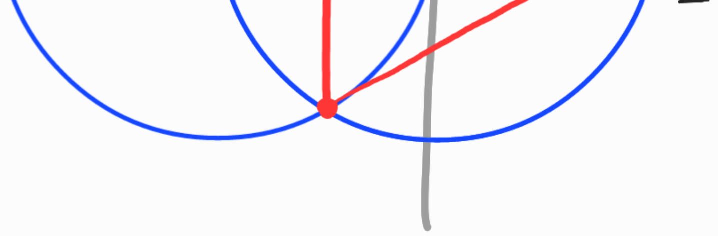
Ex ① $n = 3 = 2^{2^0} + 1$ is a Fermat prime,

so an equilateral triangle is constructible:

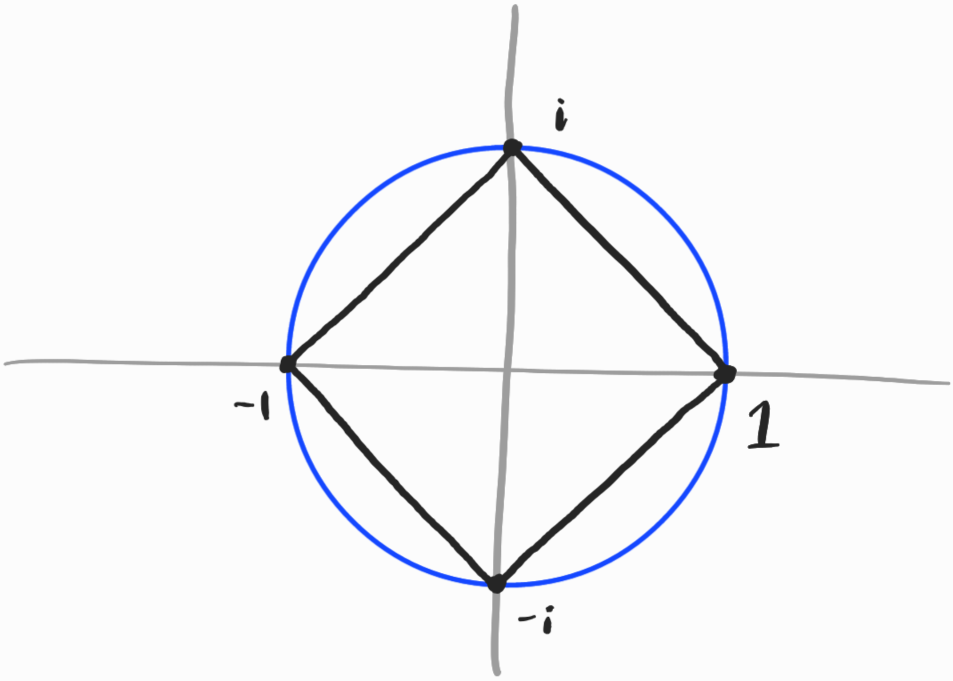


Explicitly:





② $n = 4 = 2^2$, so a square is constructible:



③ $n = 7$ is not a Fermat prime, so it is impossible to construct a regular heptagon (7-gon).

To prove Gauss' Theorem, we need to learn some Galois Theory.

Next time: exam review.