

Theorem 0.1 If the regular n -gon is constructible, then n is of the form $2^k p_1 \dots p_r$, where the $p_1 \dots p_r$ are distinct primes more than a power of 2.

Definition 0.2 Fermat Primes $= p = 1 + 2^j$

$$\frac{x^{\text{odd} \times m} + 1}{x^m + 1} \in \mathbb{Z}[x]$$

$$\implies p = 1 + 2^{2^s} \quad p = 3, 5, 17, 2^8, 65537, 2^1, 2^2, 2^4, 2^8, 2^{16}$$

E.g Regular 7-gon is not constructible.

Remark: The converse is also true.

constructible $ns = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17$

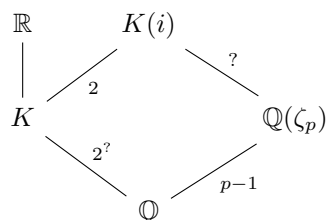
Proof: n -gon is constructible and $m|n \implies m$ -gon constructible. Therefore it's enough to show

1) if p is an odd prime, and the p -gon is constructible $\implies p$ is Fermat.

2) if p is prime and p^2 -gon is constructible $\implies p = 2$

$$1) K = \mathbb{Q}(\cos \frac{2\pi}{p}, \sin \frac{2\pi}{p})$$

p -gon constructible $\implies [K : \mathbb{Q}] = \text{power of } 2$

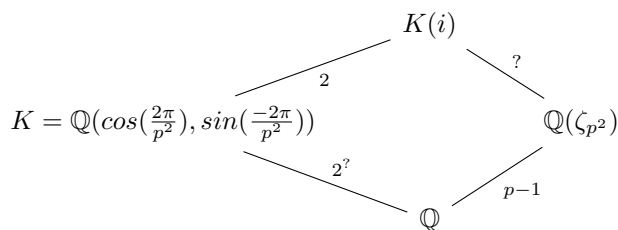


$$\therefore p-1 | 2^s$$

$\therefore p-1$ is a power of 2.

$\therefore p$ is a Fermat prime.

$$2) \zeta_p^2 \text{ is a root of } \frac{x^{p^2}-1}{x^p-1} = 1 + x^p + \dots + x^{p(p-1)}$$



$$\therefore p(p-1) | 2^s$$

$$\therefore p = 2$$

■

0.1 Splitting Fields

Definition 0.3 $F = \text{field}$,

$f(x) \in F[x]$, *non-zero*.

An extension E/F is a splitting field of $f(x)$ if

1. $f(x)$ splits over E , i.e. $f(x) = c \prod_{i=1}^n (x - \alpha_i)$, for some $c, \alpha_i \in E$
2. E is minimal w.r.t this property. i.e. $E = F(\alpha_1, \dots, \alpha_n)$

E.g.

- If $F \subset \mathbb{C}$, then

$E = F(\alpha_1, \dots, \alpha_n)$, where $\alpha_1, \dots, \alpha_n$ are the roots of $f(x) \in \mathbb{C}$, is the unique splitting field for $f(x)$ contained in \mathbb{C}

Idea: Adjoin all the roots of $f(x)$ to F .

- $f(x) = ax^2 + bx + c$ then $F(\sqrt{b^2 - 4ac})$ is a splitting field.