Theorem 0.1 *The regular n-gon is constructible iff $n = 2^r p_1 p_2 \ldots p_k$, p_i Fermat primes.*

Recall: A number α is constructible iff $\mathbb{Q}(\alpha) \supset E_j \subset \ldots \supset E_2 \supset E_1 \subset E = \mathbb{Q}$ E_{i+1}/E_i is quadratic. $E_{i+1} = E_i(\sqrt{a_i})$

A prime p is Fermat iff $p = 2^{2^a} + 1$,

$3, 5, 17, 257, 65537, \ldots$

Proof: Both sides are equivalent to $\phi(n) = 2^i$.

$\circ$ $\phi(n) = p_1^{r_1 - 1}(p_1 - 1) \ldots p_k^{r_k - 1}(p_k - 1)$;

$n = p_1^{r_1} \ldots p_k^{r_k}$

Power of 2 $\iff$ all $p_i's \neq 2$ appear with multiplicity 1 and are Fermat.

$\circ\circ$ Regular $n - gon$ constructible $\iff$ $Re(\zeta_n) = cos(\frac{2\pi}{n})$ is constructible.constructible

$cos(\frac{2\pi}{n})$ iff angle $\frac{2\pi}{n}$ constructible.

$\iff$ $\mathbb{Q}(\cos \frac{2\pi}{n}/\mathbb{Q})$ is a tower of quadratic extensions.

$\alpha = \frac{1}{2}(\zeta_n + \zeta_n^{-1}) = \frac{1}{2}(e^{2i\pi} n + e^{-2i\pi} n)$

Tower $\mathbb{Q}(\zeta_n) - (2) - \mathbb{Q}(\alpha) - - - - \mathbb{Q}$

$f(x) = (X - \zeta_n)(X - \zeta_n^{-1})$

$= x^2 - (\zeta_n + \zeta_n^{-1})x + 1$

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

$\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois because subgroups of abelian groups are normal.

Lemma: Let E/F is Galois with abelian Galois group. Then E is a tower of quadratic extensions of F $\iff$ $[E : F] =$ power of 2

$\Longrightarrow$ clear.

$\Longleftarrow$ Induction on $[E : F]$

$[E : F] = 1$ true.

$[E : F] > 1$. Choose $g \in Gal(E/F)$ of order 2.

$< g > \trianglelefteq Gal(E/F)$

$\Longrightarrow$ $E^{<g>}/F$ Galois, then use induction. ■

0.0.1 Radical Extensions

Definition 0.2 *A finite extension L/F is solvable by radicals if there is a tower of extensions $F = F_0 \hookrightarrow F_2 \hookrightarrow \ldots \hookrightarrow F_m$*

such that

- $\forall i \exists n, a \in F_i$ *s.t.* $F_{i+1} = F_i(\sqrt[n]{a})$

- $L \subseteq F_m$

Example 0.3 *$F \subset F(\sqrt[n]{a}), a \subset F$*

Let ζ_n be a primitive n^{th} root of 1.

Assume $char(F), \not| n \implies x^n - a$ has no multiple roots.

$E = F(\sqrt[n]{a}, \zeta_n)$ Galois Galois $F(\sqrt[n]{a})$ $F(\sqrt(\zeta_n))$ Galois F

$Gal(F(\zeta_n)/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$

$Gal(F(\sqrt[n]{a}, \zeta_n)/F(\zeta_n)) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$ (addition)

$Gal(F(\sqrt[n]{a}, \zeta_n)/F(\zeta_n)) =$