14.5 Cyclotomic extensions.

Inverse Galois Problem: Which finite groups occur as Galois groups $\mathrm{Gal}(K/F)$ for some K/F?

Shafarevich: Every fin solvable group is the Galois group of some $K/\mathbb{Q}$.

Open for $F = \mathbb{Q}$ in general.

Let $\zeta_n := e^{\frac{2\pi i}{n}}$ a primitive n-th root of unity.

Theorem. *For $n \in \mathbb{N}$,*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}_n^*, \cdot)$$

Note. For $n = p_1^{k_1} \dots p_\ell^{k_\ell}$ for distinct primes $p_1, \dots, p_\ell$ and $k_1, \dots, k_\ell \geq 1$,

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{k_1}}^* \times \dots \times \mathbb{Z}_{p_\ell^{k_\ell}}^*.$$

For p an odd prime and $k \geq 1$,

$$\mathbb{Z}_{p^k}^* \cong (\mathbb{Z}_{p^{k-1}(p-1)}, +)$$

For $k \geq 2$,

$$\mathbb{Z}_{2^k}^* \cong \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_2.$$

In particular, $\mathbb{Z}_n^*$ is cyclic iff $n = 1, 2, 4, p^k, 2p^k$ for p an odd prime.

Proof.

Example. $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}_5^*, \cdot) \cong (\mathbb{Z}_4, +)$

First example of a cyclic Galois group of order 4, generated by $\sigma_2 : \zeta_5 \mapsto \zeta_5^2$

$\mathrm{Fix}(\langle \sigma_2^2 \rangle) =$.

Abelian extensions.

Definition. A Galois extension K/F is *abelian* if $\mathrm{Gal}(K/F)$ is abelian.

Theorem. *Let G be a finite abelian group. Then there exist $n \in \mathbb{N}$ and $\mathbb{Q} \leq K \leq \mathbb{Q}(\zeta_n)$ such that*

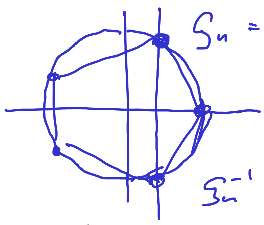
$$G \cong \mathrm{Gal}(K/\mathbb{Q}).$$

Proof: Every finite group embeds into some $(\mathbb{Z}_n^*, \cdot)$

Kronecker-Weber Theorem. *Every finite abelian extension $K/\mathbb{Q}$ is contained in some cyclotomic extension of $\mathbb{Q}$.*

Without proof. See algebraic number theory (class field theory).

Regular n-gons.



$\zeta_n = e^{2\pi i/n} = a + ib \mathrel{\hat{=}} (a,b) \in \mathbb{R}^2$

ζ_n^{-1}

Recall. A regular n-gon can be constructed by straightedge and compass iff $[\mathbb{Q}(\mathrm{Re}(\zeta_n)) : \mathbb{Q}]$ is a power of 2.

Let $a := \mathrm{Re}(\zeta_n) = \frac{1}{2}(\zeta_n + \zeta_n^{-1})$ and $K := \mathbb{Q}(a)$.
$m_{\zeta_n,K} = x^2 - 2ax + 1$.

Then $[\mathbb{Q}(\zeta_n) : K] = 2$ yields $[K : \mathbb{Q}] = \frac{\varphi(n)}{2}$.

Gauss-Wantzel **Theorem.** *TFAE for $n \in \mathbb{N}$:*

(1) *The regular n-gon can be constructed by straightedge and compass.*
(2) *$\varphi(n)$ is a power of 2.*
(3) *$n = 2^k p_1 \dots p_\ell$ for $k \in \mathbb{N}$ and distinct Fermat primes $p_1, \dots, p_\ell$.*

Definition. A *Fermat number* is of the form $2^{2^s} + 1$.

$2^1 + 1 = 3$
$2^2 + 1 = 5$
$2^4 + 1 = 17$
$2^8 + 1 = 257$
$2^{16} + 1 = 65537$

only known Fermat primes

$2^{32} + 1$ not a prime

$\vdots$