Research projects

1 Solving $\Phi_p = 0$

For p a prime, let $\mathbb{Q}(\zeta_p)$ be the smallest subfield of $\mathbb{C}$ containing $\zeta_p = e^{\frac{2\pi}{p}}$. A prime number p is called a Fermat prime if $p = 2^m + 1$

1. Let p be a Fermat prime.
   (a) Show that if p is a Fermat prime then $m = 2^n$. Find the 4 smallest Fermat primes.
   (b) Find the shape of the sub-extensions lattice of $\mathbb{Q}(\zeta_p)$.
   (c) Explain how to give an algebraic expression of ζ_p. Do it concretely for the first 3 Fermat primes.

Now p is an odd prime.

2. (a) For all sub-extensions K of $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_{11})$, find $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$.
   (b) Find the only quadratic sub-extension of $\mathbb{Q}(\zeta_p)$.

2 Inverse Galois theory

The *inverse Galois problem* over $\mathbb{Q}$ for a group G asks whether a finite group G is the Galois group of a field extension of $\mathbb{Q}$.

1. Show that $\mathbb{Z}/n\mathbb{Z}$ for all $2 \leq n \leq 12$ is the Galois group of a field extension over $\mathbb{Q}$.
2. Let $P \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p with exactly $p - 2$ real roots in $\mathbb{C}$. Show that the Galois group of the smallest subfield of $\mathbb{C}$ containing the roots of P has Galois $\mathfrak{S}_p$. Find a concrete extension with Galois group $\mathfrak{S}_5$.
3. Show that all groups of order 8 are Galois groups over $\mathbb{Q}$ (for the hardest case, consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and then $L = K\left(\sqrt{(2+\sqrt{2})(3+\sqrt{3})}\right)$)

3 Cyclotomic polynomials and finite fields

1. Find the factorization of Φ_4 in $\mathbb{F}_p[x]$ depending on the prime number p.
2. Let $\mathbb{F}_q$ be a finite field with q elements. Let n be an integer. Describe as much as you can the factorization of Φ_n in $\mathbb{F}_q[x]$.
3. Let $\ell \neq p$ be two prime numbers. Let ζ_p be $e^{\frac{2\pi}{p}}$. Let $\mathbb{Z}[\zeta_p]$ be the ring

   $$\mathbb{Z}[\zeta_p] \stackrel{\text{def}}{=} \{P(\zeta_p) \mid P \in \mathbb{Z}[x]\}.$$

   Describe the ring $\mathbb{Z}[\zeta_p]/\ell\mathbb{Z}[\zeta_p]$.