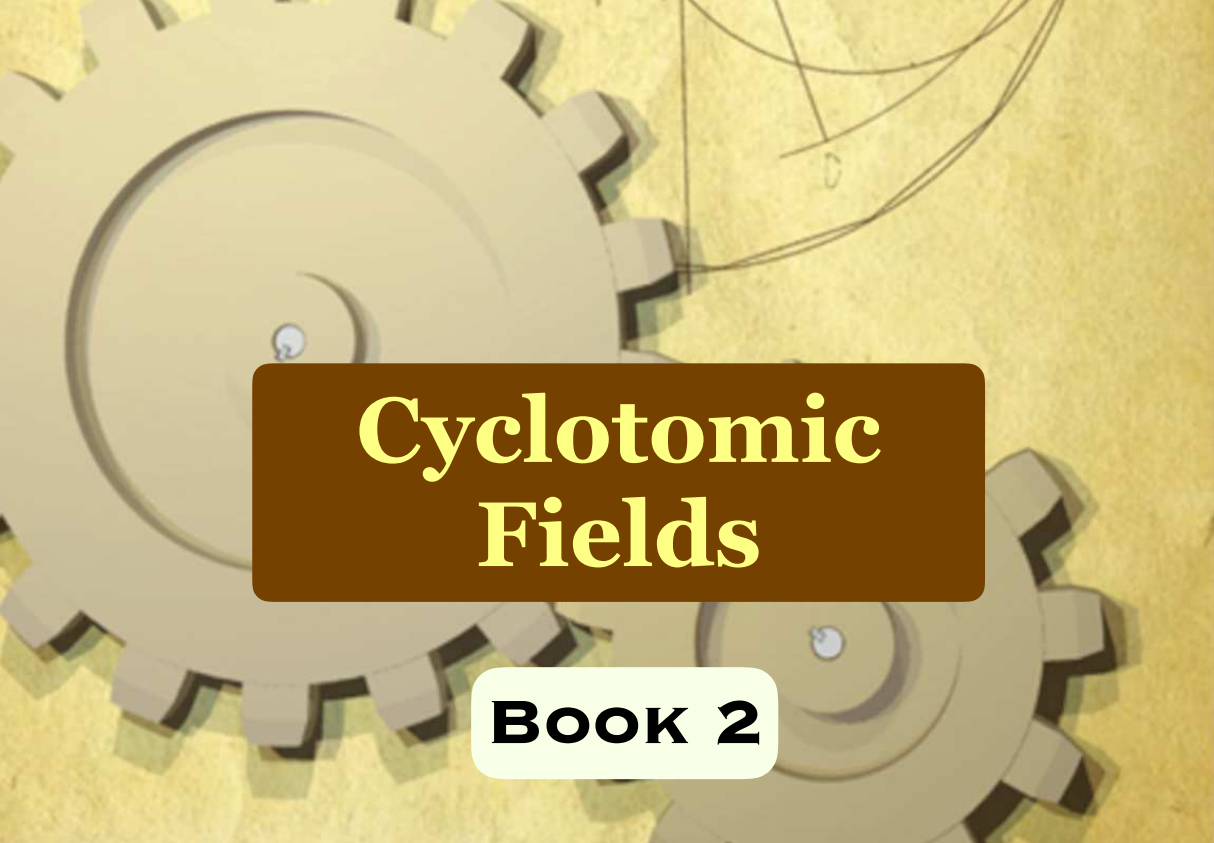




Cyclotomic Fields

BOOK 2

$$\frac{x}{e^x - 1} = 1 - \frac{1}{2}x + \frac{1}{12}x^2 - \frac{1}{720}x^4 + \frac{1}{30240}x^6 - \dots - \frac{691}{1307...0}x^{12} + \dots = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n, \quad B_n = n^{\text{th}} \text{ Bernoulli number}$$

$$g(x) = \frac{x}{e^x - 1} + \frac{1}{2}x \quad g(-x) = \frac{-x}{e^{-x} - 1} - \frac{1}{2}x = \frac{-xe^x}{1 - e^x} - \frac{1}{2}x = \frac{xe^x}{e^x - 1} - x = \frac{xe^x}{e^x - 1} - x \frac{e^x - 1}{e^x - 1} = \frac{x}{e^x - 1} = g(x)$$

even function

$$B_n: 1, -\frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, 0, -\frac{1}{42}, \dots$$

We say a ^(odd) prime p is regular if $B_2, B_4, \dots, B_{p-3}$ have no numerators divisible by p .

Otherwise p is irregular. $\downarrow e^{-1/p}$
 Heuristically, about 61% of the primes are regular
 37 is the smallest irregular prime

Hilbert Irreducibility Theorem (one form)

If $f(x, y) \in \mathbb{Q}[x, y]$ is irreducible then there exists $b \in \mathbb{Q}$ such that $f(x, b) \in \mathbb{Q}[x]$ is irreducible.

$$(x^2 + y^2)(x^2 + 3y^2) = x^4 + 4x^2y^2 + 3y^4 \text{ reducible in } \mathbb{Q}[x, y]$$

$E \supseteq \mathbb{Q}$, $[E:\mathbb{Q}] = n$ Galois. $E = \mathbb{Q}[\alpha]$, α root of $m(x) \in \mathbb{Q}[x]$ irreducible of degree n .

$G = \text{Aut } E = \text{Galois group of } E$. G transitively permutes the n roots of $m(x)$.

If $n=3$ then $G \cong C_3$. $m(x) = x^3 + x^2 - 2x - 1$, $E \subset \mathbb{Q}[\zeta_7]$.

Usually if $m(x) \in \mathbb{Q}[x]$ is irreducible of degree 3 then $\mathbb{Q}[\alpha] \supset \mathbb{Q}$ is not Galois; its Galois closure has degree 6 over $\mathbb{Q}$ with Galois group S_3 permuting the three roots of $m(x)$ in all $3! = 6$ ways.

Inverse problem of Galois theory: Given G , find an extension $E \supseteq \mathbb{Q}$ having G as its group of automorphisms.

Try to realize $G \leq S_n$ (transitive subgroup) as the Galois group of $E \supset \mathbb{Q}$, $E = \mathbb{Q}[\alpha_1, \dots, \alpha_n]$,
 $m(x) \in \mathbb{Q}[x]$ of degree n , $m(x) = (x - \alpha_1) \cdots (x - \alpha_n)$

If we can find an extension $\mathbb{E} \supset \mathbb{Q}(t)$ then specialize t to some rational number
hope to get a finite extension of $\mathbb{Q}$ with ^{t indeterminate i.e. transcendental} given Galois group.

A Hadamard matrix of order n is an $n \times n$ matrix H with entries ± 1 such that $HH^T = nI$ (i.e. $H^TH = nI$
i.e. $H^T = \frac{1}{n}H$ i.e. $\frac{1}{\sqrt{n}}H$ is real orthogonal).

$$[1], [-1], \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \dots$$

For $n \geq 1$, if there exists a Hadamard matrix of order n , then $n=1$ or 2 or $n \equiv 0 \pmod{4}$.

Question: If $n=4k$ for $k \geq 1$, does there necessarily exist a Hadamard matrix of order n ?

The smallest open case was for $n=668$ until 2026.

If $n \geq 2$ then order n Hadamard requires n even since the dot product of the first two rows is $\equiv n \pmod{2}$.

If $n \geq 3$ then we actually require $n \equiv 0 \pmod{4}$.