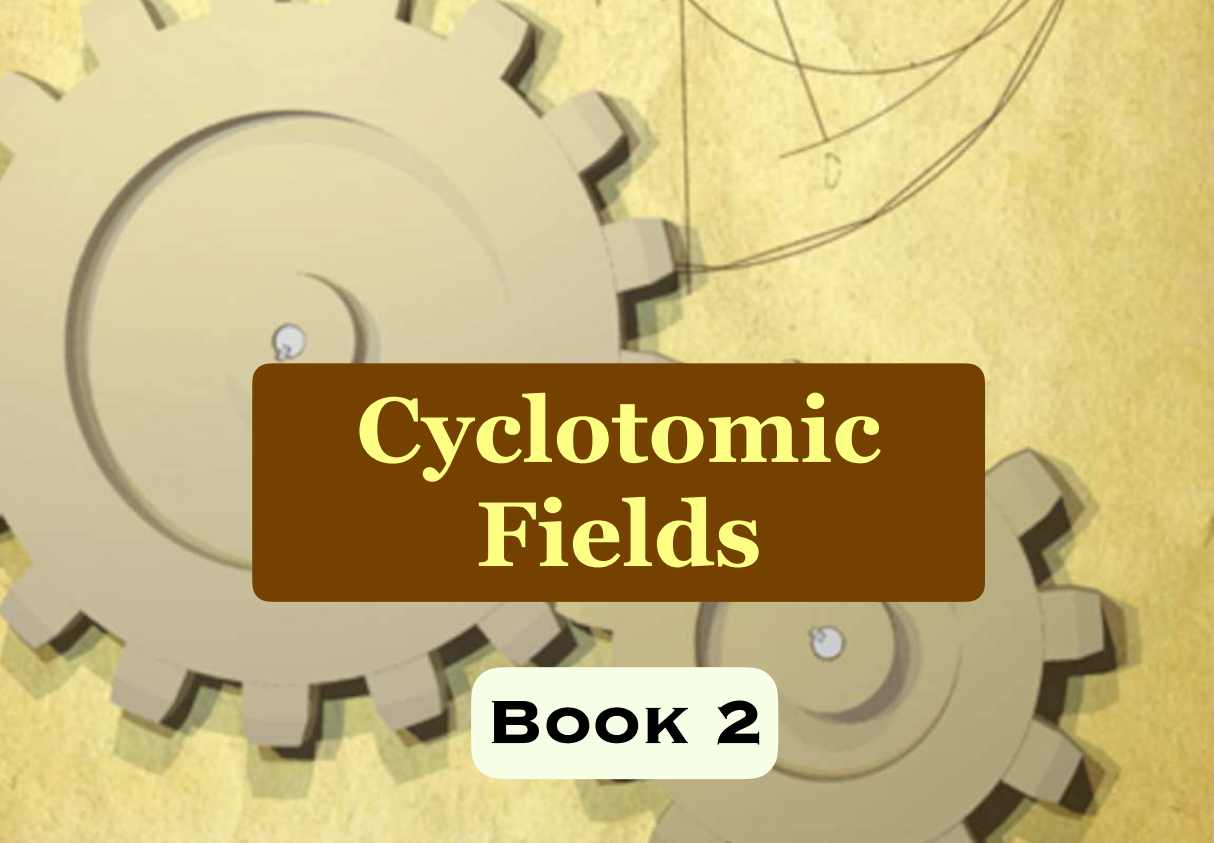




Cyclotomic Fields

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. $\leftarrow e^{-1/p}$

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 .

$G = \text{Aut } E =$ 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. $H^{-1} = \frac{1}{n}H^T$ i.e. $\frac{1}{\sqrt{n}}H$ is real orthogonal).

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

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 $n \equiv 0 \pmod{4}$.

Let H be a Hadamard matrix of order $n \geq 3$.

First three rows:

$$\begin{array}{ccccccc} + & + & + & + & \dots & \dots & + & + & + & \dots & \dots & + \\ + & + & + & + & \dots & \dots & + & - & - & \dots & \dots & - \\ + & \dots & \dots & + & - & \dots & - & + & \dots & + & - & \dots & - \\ \hline & l & & k-l & & k-l & & l & & & & \end{array}$$

$$\underbrace{\hspace{10em}}_k \quad \underbrace{\hspace{10em}}_k$$

$$n = 2k$$

$$l - (k-l) - (k-l) + l = 4l - 2k = 0 \Rightarrow n = 2k = 4l$$

Circulant matrix: $\begin{bmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_1 & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \dots & a_0 \end{bmatrix}$ each row is a cyclic shift of the previous row

+	+	+	+	+	+	+	+
+	+	+	-	+	-	-	-
+	-	+	+	-	+	-	-
+	-	-	+	+	-	+	-
+	-	-	-	+	+	-	+
+	+	-	-	-	+	+	-
+	-	+	-	-	-	+	+
+	+	-	+	-	-	-	+

$$\begin{aligned} + &= 1 \\ - &= -1 \end{aligned}$$

Terry Tao
Mathematics in the Age of AI
preprint: arXiv
YouTube

7x7 circulant matrix

Can replace 7 by any prime $p \equiv 3 \pmod{4}$ or any $q \equiv 3 \pmod{4}$, prime power eg.

$$\begin{bmatrix} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & - & - & + \end{bmatrix}$$

$$\text{or } \begin{bmatrix} - & + & + & + \\ + & - & + & + \\ + & + & - & + \\ + & + & + & - \end{bmatrix} \quad [+]$$

There are many invalid claims to have proved the Hadamard Matrix Conjecture.

$$n = 4k$$

A, B, C, D are $k \times k$ circulant matrices with entries ± 1

Bernard Schmidt is the expert.

A, B, C, D commute with each other
 A, B, C, D symmetric

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}$$

$$HH^T = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix} \begin{bmatrix} A & -B & -C & -D \\ B & A & -D & -C \\ C & -D & A & B \\ D & C & -B & A \end{bmatrix} = \begin{bmatrix} A^2+B^2+C^2+D^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\text{Need } A^2+B^2+C^2+D^2 = nI = 4kI$$

Complex Hadamard matrix of order n : $n \times n$ matrix H with entries h_{ij} , $|h_{ij}| = 1$.

such that $HH^* = H^*H = nI$. These exist for all $n \geq 1$.

$$\text{eg. } F = F_n, \quad h_{ij} = \omega^{ij} \quad 0 \leq i, j \leq n-1$$

Using blocks of circulant matrices to construct new Hadamard matrices: why?

+	+	-	+	-	-	-
-	+	+	-	+	-	-
-	-	+	+	-	+	-
-	-	-	+	+	-	+
+	-	-	-	+	+	-
-	+	-	-	-	+	+
+	-	+	-	-	-	+

$$= I + C - C^2 + C^3 - C^4 - C^5 - C^6 \in \mathbb{Q}[C]$$

$$\text{where } I = I_7, \quad C = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ & & & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad C^7 = I$$

$\mathbb{Q}[x]$ = algebra of polynomials in x with rational (number) coefficients

algebra = ring + vector space over $\mathbb{Q}$

$\mathbb{Q}[x] \xrightarrow{\phi} \mathbb{Q}[C]$ algebra homomorphism; surjective
infinite-dimensional 7-dimensional

$\ker \phi \subseteq \mathbb{Q}[x]$ is an ideal. It is a subspace such that $f(x)g(x) \in \ker \phi$ for all $g(x) \in \ker \phi$ or $f(x) \in \mathbb{Q}[x]$.

$\ker \phi = (x^7 - 1)$ = principal ideal generated by $x^7 - 1$
 $= \{ f(x)(x^7 - 1) : f(x) \in \mathbb{Q}[x] \}$.

First Isomorphism Theory: $\mathbb{Q}[C] \cong \mathbb{Q}[x] / (x^7 - 1) = \{ a_0 + a_1 x + \dots + a_6 x^6 : a_i \in \mathbb{Q} \}$
 with "wrap-around" $x^7 = 1$.

If G is cyclic of order 7, say multiplicative, $G = \langle g : g^7 = 1 \rangle = \{ 1, g, g^2, \dots, g^6 \}$

$$\mathbb{Q}[G] = \{ a_0 + a_1 g + a_2 g^2 + \dots + a_6 g^6 : a_i \in \mathbb{Q} \}$$

$$g^i g^j = g^{i+j} \text{ exponents mod 7.}$$

the group algebra of G over $\mathbb{Q}$
 i.e. the rational group algebra of G

Because $\mathbb{Q}[G]$ is a commutative algebra, it can be "simultaneously diagonalized"

C has n eigenvalues $1, \xi, \xi^2, \dots, \xi^6$ in $\mathbb{Q}[\xi] = E \cong \mathbb{Q}$
 with eigenvectors $v_i = \begin{bmatrix} 1 \\ \xi^i \\ \xi^{2i} \\ \vdots \\ \xi^{6i} \end{bmatrix}$, $C v_i = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \dots & 0 \end{bmatrix} \begin{bmatrix} 1 \\ \xi^i \\ \xi^{2i} \\ \vdots \\ \xi^{6i} \end{bmatrix} = \begin{bmatrix} \xi^i \\ \xi^{2i} \\ \vdots \\ \xi^{6i} \\ 1 \end{bmatrix} = \xi^i v_i$
 $v_0 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$, $v_1 = \begin{bmatrix} 1 \\ \xi \\ \xi^2 \\ \vdots \\ \xi^6 \end{bmatrix}$, $\dots$ basis of eigenvectors of C .

After conjugating by H (complex Hadamard of order 7) $C \rightsquigarrow \begin{bmatrix} \xi & \xi^2 & 0 \\ 0 & \xi^3 & \xi^6 \end{bmatrix}$

$$\mathbb{Q}[C] \cong \bigoplus_{i=0}^6 \mathbb{Q} \cong \mathbb{Q}^7.$$

Cyclic of order 7
 $G = \langle g \rangle = \{1, g, g^2, \dots, g^6\}$
 $g^7 = 1$

In $\mathbb{Q}[G]$, the element $\delta = 1 + g + g^3$ satisfies a nice identity: $D = \{1, g, g^3\} \subset G$ is a difference set: every $x \in G$, $x \neq 1$, is uniquely expressible as $x = d_1 d_2^{-1}$, $d_1, d_2 \in D$.

$$\begin{aligned} g \cdot 1^{-1} &= g \\ g^3 \cdot 1^{-1} &= g^3 \\ 1 \cdot g^{-1} &= g^6 \\ 1 \cdot (g^3)^{-1} &= g^4 \\ g \cdot (g^3)^{-1} &= g^5 \\ g^3 \cdot g^{-1} &= g^2 \end{aligned}$$

$$\begin{aligned} 1 \cdot 1^{-1} &= 1 \\ g \cdot g^{-1} &= 1 \\ g^3 \cdot (g^3)^{-1} &= 1 \end{aligned}$$

$$\delta \delta^* = (1 + g + g^3)(1 + g^{-1} + g^{-3}) = 2 + \tau,$$

$\mathbb{Z}G = \mathbb{Z}[G] \leftarrow$ integral group algebra $\tau = \sum_{g \in G} g$
 $\mathbb{Q}G = \mathbb{Q}[G] \leftarrow$ rational group algebra.
 $\mathbb{Q}G = \mathbb{Q}[G]$ is an algebra with basis G

$$\text{If } \alpha = \sum_{g \in G} a_g g, \quad g \in \mathbb{Q}$$

$$\text{then } \alpha^* = \sum_{g \in G} a_g g^{-1}$$

9 ways to take $d_1 d_2^{-1}$, $d_1, d_2 \in D$

If G is any finite group of order $v = |G|$,
 a (v, k, λ) -difference set in G is a subset $D \subset G$
 of size $|D| = k$ such that every nonidentity element of G can be expressed as $d_1 d_2^{-1}$, $d_1, d_2 \in D$, $d_1 \neq d_2$ in λ ways.

In a finite group G , $|G|=v$, a (v,k,r) -difference set is a subset $D \subset G$ such that $|D|=k$ and every nonidentity element $x \in G$ can be expressed as $x = d_1 d_2^{-1}$, $d_1, d_2 \in D$, $d_1 \neq d_2$ in exactly r ways.

In order for a difference set to exist, the parameters (v,k,r) must satisfy certain necessary conditions.

Count in two different ways the number of pairs $(d_1, d_2) \in D^2$:

$$k^2 = k + r(v-1) \Rightarrow k^2 - k = k(k-1) = r(v-1).$$

The condition for $D \subset G$ to be a difference set is expressible in the language of group rings/algebras.

Example:

$(7,3,1)$ -difference set in a cyclic group of order 7.

Consider $S = \sum_{d \in D} d \in \mathbb{Z}G$ and $\gamma = \sum_g g \in \mathbb{Z}G$.

eg. in $G = \langle g : g^7 = 1 \rangle$, $D = \{1, g, g^3\}$, $\gamma = 1 + g + g^2 + g^3 + g^4 + g^5 + g^6$,

$$S = 1 + g + g^3, \quad S^* = 1 + g^{-1} + g^{-3} = 1 + g^4 + g^6$$

$$SS^* = (1 + g + g^3)(1 + g^4 + g^6) = 3 + g + g^2 + g^3 + g^4 + g^5 + g^6 = 2 + \gamma$$

In the general case: $SS^* = n + r\gamma$ where $n = k - r$

$$= \underbrace{n+r}_k + r \sum_{1 \neq g \in G} g$$

If G were written additively as

$$G = \{0, 1, 2, 3, 4, 5, 6\} \text{ then } D = \{0, 1, 3\}$$

Every nonidentity $x \in G$ is expressible as $x = d_1 - d_2$ for exactly one pair $(d_1, d_2) \in D^2$, $d_1 \neq d_2$.

How do we search for solutions of $\delta\delta^+ = n + r\gamma$ in $\mathbb{Z}G$ or $\mathbb{Q}G$?

As a vector space, $\dim \mathbb{Q}G = |G| = r$

As an algebra over $\mathbb{Q}$, if G is abelian then $\mathbb{Q}G \cong \mathbb{Q}^r = \underbrace{\mathbb{Q} \oplus \mathbb{Q} \oplus \dots \oplus \mathbb{Q}}_{r \text{ times}}$

There are many ^{algebra} homomorphisms $\mathbb{Q}G \rightarrow \mathbb{C}$ ("linear" characters)

i.e. maps $\chi: \mathbb{Q}G \rightarrow \mathbb{C}$

$$\chi(a\alpha + b\beta) = a\chi(\alpha) + b\chi(\beta)$$

$$a, b \in \mathbb{Q}$$

$$\alpha, \beta \in \mathbb{Q}G$$

$$\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$$

$$\chi(1) = 1$$

eg. $\chi_i: \mathbb{Q}^r \rightarrow \mathbb{C}$

$$(x_1, \dots, x_r) \mapsto x_i$$

Assuming G is abelian, G has exactly $r = |G|$ algebra homomorphisms

$$\chi_i: \mathbb{Q}G \rightarrow \mathbb{C}$$

For $\alpha, \beta \in \mathbb{Q}G$, $\alpha = \beta$ iff $\chi(\alpha) = \chi(\beta)$ for all $\chi \in \hat{G} = \{ \text{algebra homomorphisms } \mathbb{Q}G \rightarrow \mathbb{C} \}$

If $G = \{1, g\}$, $g^2 = 1$

$$\chi_0(1) = \chi_0(g) = 1$$

$$\chi_1(1) = 1, \chi_1(g) = -1$$

$$\chi_0(a + bg) = a + b$$

$$\chi_1(a + bg) = a - b$$

Apply these homomorphisms to the equation $\delta\delta^+ = n + r\gamma$

Theorem Let G be an abelian mult. gp. of order v and consider a nonempty subset $D \subset G$, $|D| = k < v$ and $S = \sum_{d \in D} d \in \mathbb{Z}G$. Then

D is a (v, k, r) -diff. set in G iff $k^2 - rv = n := k - r$ and

$|\chi(S)| = \sqrt{n}$
for every nontrivial $\chi \in \hat{G}$.