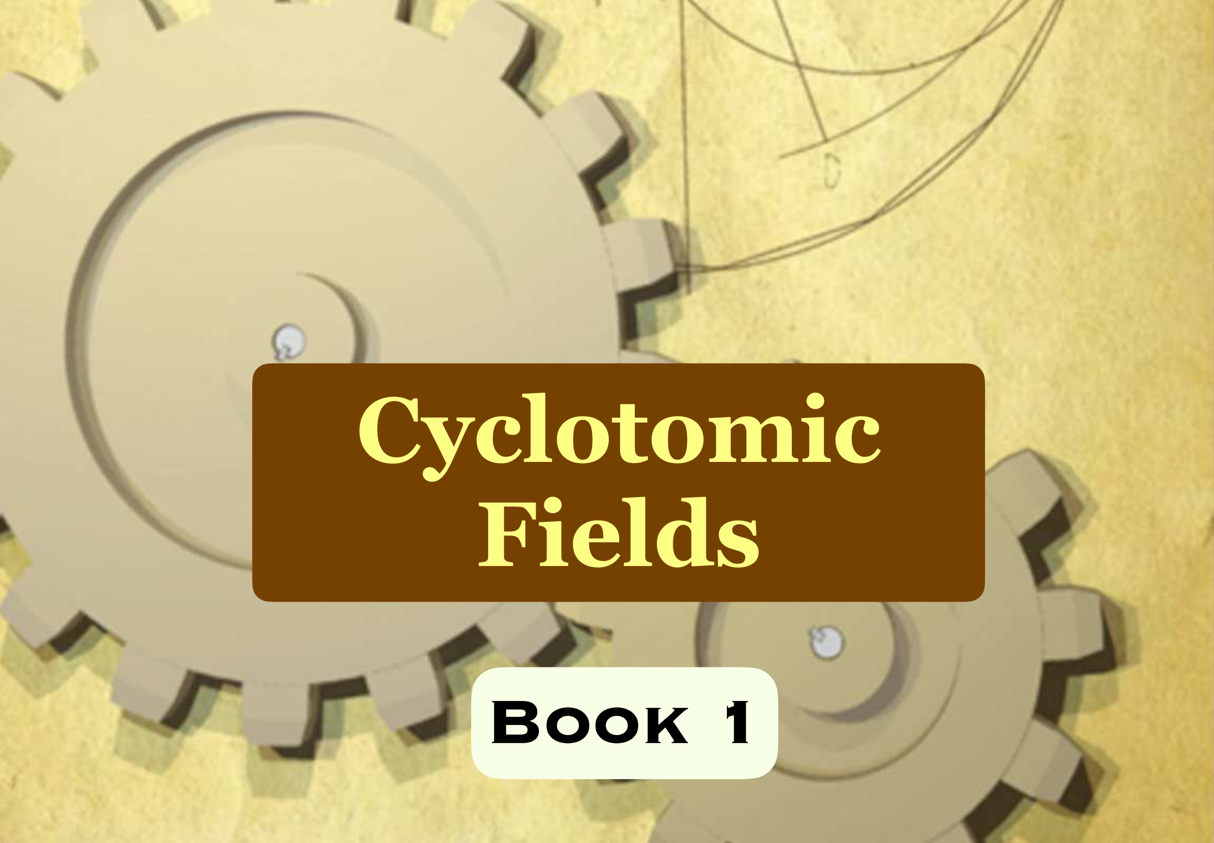
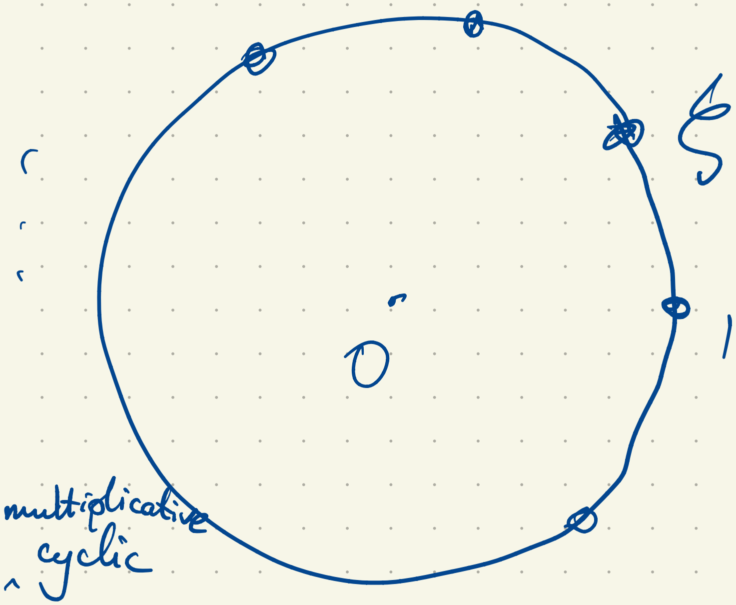


Cyclotomic Fields

Book 1

A (complex) n^{th} root of unity is a value $\zeta \in \mathbb{C}$ satisfying $\zeta^n = 1$.

$$\boxed{\begin{array}{l} \zeta \ \xi \qquad \phi \ \xi \ \pi \ \chi \\ \zeta \ \beta \ \theta \end{array}}$$



$\zeta = e^{2\pi i/n}$

Solutions of $z^n = 1$ form a multiplicative cyclic group of order n.

There are $\phi(n)$ primitive n^{th} roots of unity.

Euler's totient function

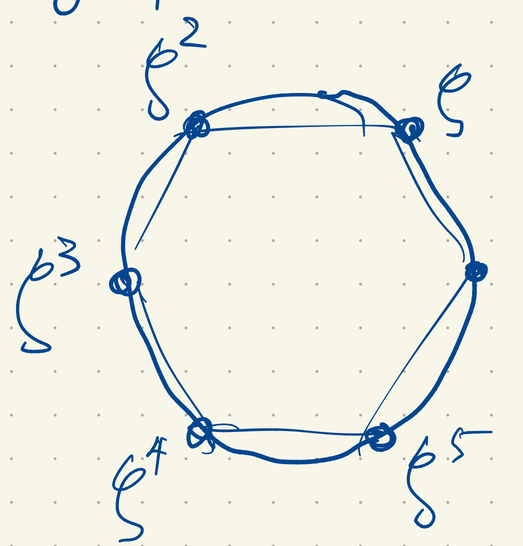
$\phi(n)$ = number of generators in any cyclic group of order n.

eg. $n = 6$ $\quad \phi(6) = 2$.

$\phi(n) = \left| \{ k \in \{1, 2, \dots, n\} : \gcd(k, n) = 1 \} \right|$

1, 5 relatively prime to 6.

All sixth roots of unity are ζ^k, $1 \le k \le n$. $\quad -1 = \zeta^3$



A <u>cyclotomic field</u> is a field $\mathbb{Q}[\zeta]$ where $\zeta \in \mathbb{C}$ is a root of unity.

$\zeta^n = 1 \implies 1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = 0$

$$z^n - 1 = (z-1)(1 + z + z^2 + \cdots + z^{n-1})$$

$$n=6: \quad z^6 - 1 = \underbrace{(z-1)}_{\Phi_1(z)}\underbrace{(z+1)}_{\Phi_2(z)}\underbrace{(z^2+z+1)}_{\Phi_3(z)}\underbrace{(z^2-z+1)}_{\Phi_6(z)}$$

(factorization into irreducible factors in $\mathbb{Q}[x]$ or $\mathbb{Z}[x]$)

Roots: 1, $\quad -1 = \zeta^3$, $\quad \zeta^2, \zeta^4$, $\quad \zeta, \zeta^5$

primitive sixth roots of 1.

$\Phi_n(z)$ = minimal poly. of $\zeta = e^{2\pi i/n}$ over $\mathbb{Q}$ (or over $\mathbb{Z}$)
(simplest monic poly. with rational coefficients having ζ as a root)

$$z^n - 1 = \prod_{\substack{d \mid n \\ d \geq 1}} \Phi_d(z) \qquad \text{product over all positive integer divisors of } n.$$

Divisors of 6 are $\pm 1, \pm 2, \pm 3, \pm 6$
Positive divisors of 6 are $1, 2, 3, 6$.

$$\Phi_n(z) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n) = 1}} (z - \zeta^k) \qquad \text{has as its roots the primitive } n^{th} \text{ roots of } 1.$$

$\mathbb{Q}[\zeta_n]$ = { polynomials in ζ with coefficients in $\mathbb{Q}$ }
= { linear combinations of $1, \zeta, \zeta^2, \ldots$ with rational coefficients }
= { linear combinations of $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ with coefficients in $\mathbb{Q}$ }

$\zeta = \zeta_n = e^{2\pi i/n}$