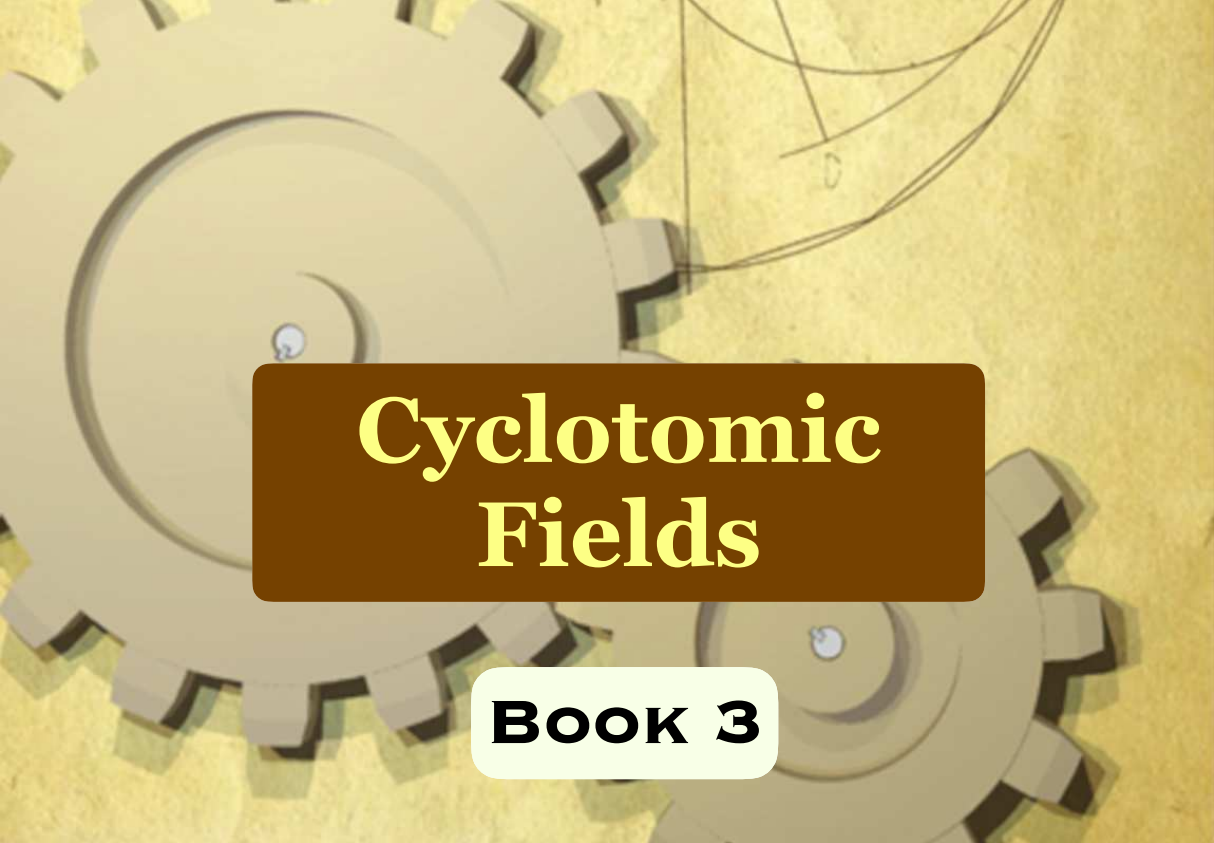

Cyclotomic Fields
Book 3

$q = p^e$, p prime, $e \geq 1$

$\mathbb{F}_q \supseteq \mathbb{F}_p$ $\quad \mathbb{F}_q = \mathbb{F}_p[\theta]$, θ root of $m(x) \in \mathbb{F}_p[x]$ irreducible of degree e.

$[\mathbb{F}_q : \mathbb{F}_p] = e$ $\quad \mathrm{Aut}\, \mathbb{F}_q = \{1, \sigma, \sigma^2, \cdots, \sigma^{e-1}\}$ where $\sigma(a) = a^p$.

$\sigma(ab) = (ab)^p = a^p b^p$

$\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b)$

$\sigma : \mathbb{F}_q \to \mathbb{F}_q$ is $\mathbb{F}_p$-linear

If $\alpha \in \mathbb{F}_q$ and $c \in \mathbb{F}_p$ then $\sigma(c) = c^p = c$ (Fermat's Little Theorem or Lagrange's Thm)

$\sigma(c\alpha) = \sigma(c)\sigma(\alpha) = c\,\sigma(\alpha)$

σ is one-to-one:

If $\alpha, \beta \in \mathbb{F}_q$ then $\sigma(\alpha - \beta) = (\alpha - \beta)^p = 0 \iff \alpha - \beta = 0$.

$\sigma(\alpha) = \alpha^p = 0 \iff \alpha = 0$ So σ has null space $\{0\}$ so σ is 1-to-1. σ is one-to-one.

$\sigma^k(a) = (((a^p)^p)\cdots)^p = a^{p^k}$, $\quad k = 0, 1, 2, \cdots, e-1$

$\sigma^e(a) = a = a^{p^e} = a^q = a$

If $1 \leq k \leq e-1$ then $\sigma^k \neq 1$ = identity. (If $\sigma^k = 1$ then the polynomial $x^{p^k} - x$ has $q = p^e$ roots in $\mathbb{F}_q$

$G = \mathrm{Aut}\, \mathbb{F}_q = \langle \sigma : \sigma^e = 1 \rangle$ = cyclic of order e

$|\mathrm{Aut}\, \mathbb{F}_q| = [\mathbb{F}_q : \mathbb{F}_p] = e$ So the extension is Galois

Subgroups of G $\overset{1:1}{\longleftrightarrow}$ subfields of $\mathbb{F}_q$

$G \longleftrightarrow \mathbb{F}_p$

$$\mathbb{F}_p = \{\alpha \in \mathbb{F}_q : \underbrace{\sigma(\alpha) = \alpha}_{\alpha^p = \alpha}\}$$

$\alpha^\sigma = \sigma(\alpha)$

$\sigma(\mathrm{Tr}(\alpha))$

$\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$

If $\alpha \in \mathbb{F}_q$ then $\sigma(\alpha)$ has the same char. poly and min. poly. ($\sigma(\alpha)$ is an algebraic conjugate of α) and in particular $\mathrm{Tr}(\sigma(\alpha)) = \mathrm{Tr}(\alpha)$.

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{e-1}} = \sum_{g \in G} \alpha^g = \sum_{i=0}^{e-1} \alpha^{\sigma^i}$$

$$\mathrm{Tr}(\alpha)^\sigma = \sum_{g \in G} \alpha^{g\sigma} = \sum_{g \in G} \alpha^g = \mathrm{Tr}(\alpha) \quad \text{so } \mathrm{Tr}\,\alpha \in \mathbb{F}_p.$$

A finite field $\mathbb{F}_q$, $q = p^e$ has

- an additive group: addition in an e-dimensional vector space over $\mathbb{F}_p$
  (an elementary abelian group $\underbrace{C_p \times C_p \times \cdots \times C_p}_{e}$)
- $\mathbb{F}_q^\times$ is a cyclic multiplicative group of order $q-1$.

Gauss sums keep track of how the two operations mesh with each other.

The field $\mathbb{F}_q$ has two kinds of characters $\mathbb{F}_q \to \mathbb{C}$

An additive character of $\mathbb{F}_q$ is a map $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ (nonzero) such that $\psi(x \overset{\text{addition in } \mathbb{F}_q}{+} y) = \psi(x) \overset{\text{multiplication in } \mathbb{C}^\times}{\psi}(y)$ for all $x, y \in \mathbb{F}_q$.
(homomorphism)

Note: $\psi(0) = 1$ and $\psi(\alpha)^p = \psi(\underbrace{\alpha + \alpha + \cdots + \alpha}_{p}) = \psi(0) = 1$

So $\psi(\alpha) \in \{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$.

A multiplicative character of $\mathbb{F}_q$ is a map $\chi : \mathbb{F}_q \to \mathbb{C}$ satisfying $\chi(0) = 0$ and $\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$ for all nonzero $\alpha, \beta \in \mathbb{F}_q$.

Also $\chi(1) = 1$, i.e. $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ is a homo. of groups
ie (linear) characters.