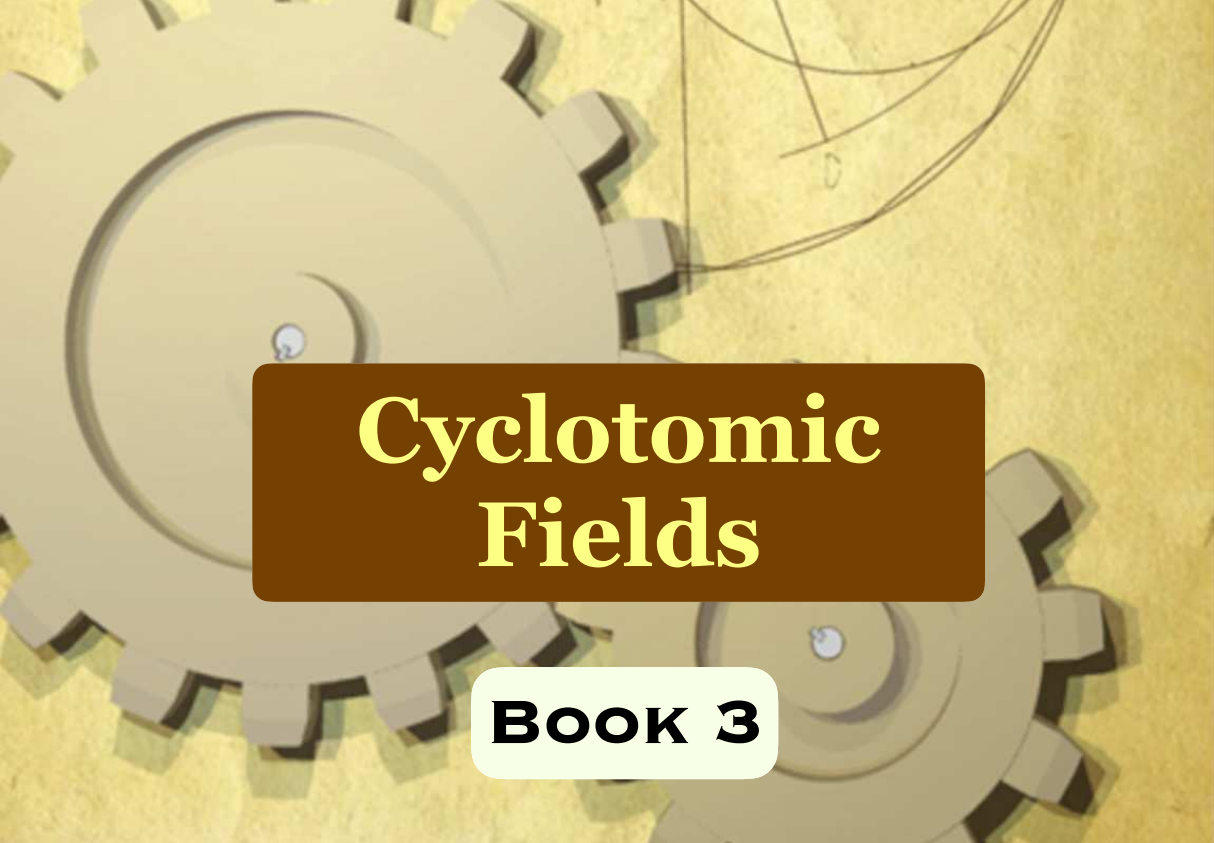

Cyclotomic Fields
Book 3

$q = p^e$, 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 $\psi(x+y) = \psi(x)\psi(y)$ for all $x, y \in \mathbb{F}_q$. (addition in $\mathbb{F}_q$, multiplication in $\mathbb{C}^\times$; homomorphism)

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

So $\psi(\alpha) \in \{1, \xi_p, \xi_p^2, \ldots, \xi_p^{r'}\}$.

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.

Exception: The principal multiplicative character $\chi_0(\alpha) = 1$ for all $\alpha \in \mathbb{F}_q$.

$$\chi_0(0) = \chi_0(0 \cdot 1) = \chi_0(0)\chi_0(1)$$

The principal additive character

$\psi_0(\alpha) = 1$. (for all $\alpha \in \mathbb{F}_q$).

Every additive character satisfies $\psi(0) = 1$ because

$\psi(\alpha) = \psi(0+\alpha) = \psi(0)\psi(\alpha)$



$\lim_{x \to 0^+} x^x = 1$

x^y

What is 0^0? $0^0 = 1$ but why?

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i$

$f(0) = a_0 = a_0 0^0 \Rightarrow 0^0$

$\prod_{s \in S}$ = product of all elements of S

$\sum_{s \in S}$ = sum of all elements of S

$\sum_{s \in \emptyset} = 0$

$S \cap T = \emptyset$

$$\sum_{x \in S \cup T} x = \sum_{x \in S} x + \sum_{x \in T} x$$

$$\sum_{x \in T} = \left(\sum_{x \in \emptyset}\right) + \sum_{x \in T} \quad (\text{where } \textstyle\sum_{x \in \emptyset} = 0)$$

$$\prod_{x \in S \cup T} x = \left(\prod_{x \in S} x\right)\left(\prod_{x \in T} x\right)$$

$$\prod_{x \in T} x = \left(\prod_{x \in \emptyset} x\right)\left(\prod_{x \in T} x\right)$$

The most important additive character is $\psi_1(\alpha) = \zeta^{\mathrm{Tr}\alpha}$ where $\mathrm{Tr}: \mathbb{F}_q \to \mathbb{F}_p$

$\psi_1: \mathbb{F}_q \to \mathbb{C}^\times$ $\quad \mathrm{Tr}(\alpha+\beta) = \mathrm{Tr}\alpha + \mathrm{Tr}\beta$.

$\psi_1(\alpha+\beta) = \zeta^{\mathrm{Tr}(\alpha+\beta)} = \zeta^{\mathrm{Tr}\alpha+\mathrm{Tr}\beta} = \zeta^{\mathrm{Tr}\alpha}\zeta^{\mathrm{Tr}\beta}$

$= \psi_1(\alpha)\psi_1(\beta)$.

Fix $\zeta = \zeta_p = e^{2\pi i/p}$ primitive p^{th} root of unity in $\mathbb{C}$.

$\mathbb{F}_p \to \mathbb{C}$

$a \mapsto \zeta^a$

More generally, fix $\gamma \in \mathbb{F}_q$; define

$$\psi_\gamma(\alpha) = \zeta^{\mathrm{Tr}(\gamma\alpha)}$$

$$\psi_\gamma(\alpha+\beta) = \zeta^{\mathrm{Tr}(\gamma(\alpha+\beta))} = \zeta^{\mathrm{Tr}(\gamma\alpha+\gamma\beta)} = \zeta^{\mathrm{Tr}(\gamma\alpha)+\mathrm{Tr}(\gamma\beta)} = \zeta^{\mathrm{Tr}(\gamma\alpha)}\zeta^{\mathrm{Tr}(\gamma\beta)} = \psi_\gamma(\alpha)\psi_\gamma(\beta).$$

When $\gamma = 0 \in \mathbb{F}_q$, this gives us the principal character ψ_0 as a special case.
There are exactly q additive characters of $\mathbb{F}_q$ and these are all of them.

Now consider a multiplicative character $\chi: \mathbb{F}_q \to \mathbb{C}$, i.e. $\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$ for all $\alpha, \beta \in \mathbb{F}_q$.

The principal multiplicative character $\chi_0(\alpha) = 1$.

There are $q-1$ nonprincipal mult characters χ : $\chi(0) = 0$

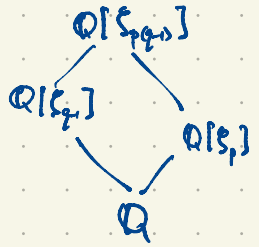
$\chi(\alpha) \neq 0$ for $\alpha \neq 0$.

For $0 \neq \alpha \in \mathbb{F}_q$, $\alpha^{q-1} = 1$ so $\chi(\alpha)^{q-1} = \chi(\alpha^{q-1}) = \chi(1) = 1$. So $\chi(a) \in \mathbb{Q}[\zeta_{q-1}]$

Gauss sums $G(\chi, \psi) = \sum_{x \in E} \chi(x)\psi(x) \in \mathbb{Q}[\zeta_p, \zeta_{q-1}]$ $\quad E = \mathbb{F}_q$, $q = p^e$

$= \mathbb{Q}[\zeta_{p(q-1)}]$

(χ: mult. char. of E; ψ: additive character of E)



Let $\gamma \in E$ be primitive i.e.

$E = \{0, 1, \gamma, \gamma^2, \cdots, \gamma^{q-2}\}$

$E^\times$ is cyclic of order $q-1$.

$\alpha = \gamma^k$ for some $k \in \{0, 1, 2, \cdots, q-2\}$

$\chi(\alpha) = \chi(\gamma)^k$

Look at $G(\chi_0,\psi_0)$, $G(\chi_0,\psi)$, $G(\chi,\psi_0)$, $G(\chi,\psi)$ where $\chi\neq\chi_0$, $\psi\neq\psi_0$.

$$G(\chi_0,\psi_0)=\sum_{x\in E}\underbrace{\chi_0(x)}_{1}\underbrace{\psi_0(x)}_{1}=q.$$

$$G(\chi_0,\psi)=\sum_{x\in E}\psi(x)=\sum_{x\in E}\psi(a+x)=\sum_{x\in E}\psi(a)\psi(x)=\psi(a)\sum_{x\in E}\psi(x)\Rightarrow G(\chi_0,\psi)=0.$$

Fix $a\in E$: there is at least one $a\in E$ with $\psi(a)\neq 1$

Similarly $G(\chi,\psi_0)=0$

$$|G(\chi,\psi)|^2=\sum_{x,y\in E}\chi(x)\psi(x)\overline{\chi(y)\psi(y)}=\sum_{\substack{x,y\neq 0\\ \text{in } E}}\chi(x)\overline{\chi(y)}\,\psi(x)\overline{\psi(y)}=q-1+\sum_{\substack{x,y\neq 0\\ x\neq y}}\underbrace{\chi(x)\overline{\chi(y)}}\,\underbrace{\psi(x)\overline{\psi(y)}}$$

$$=q-1+\sum_{\substack{x,y\neq 0\\ x\neq y}}\chi(\underbrace{\tfrac{x}{y}}_{u})\psi(\underbrace{x-y}_{v})$$

$$x=\frac{uv}{u-1},\quad y=\frac{v}{u-1}$$

$$\frac{\chi(x)}{\chi(y)}=\chi\left(\frac{x}{y}\right)\qquad\frac{\psi(x)}{\psi(y)}=\psi(x-y)$$

$$=q-1+\sum_{\substack{u\neq 1\\ v\neq 0}}\chi(u)\psi(v)=q-1+\left(\sum_{u\neq 1}\chi(u)\right)\left(\sum_{v\neq 0}\psi(v)\right)$$

$$\sum_{u\in E}\chi(u)=0\qquad\sum_{v\in E}\psi(v)=0$$

$$=q-1+(-1)(-1)=q.$$

$$\boxed{|G(\chi,\psi)|=\sqrt{q}}.$$

Now let χ, χ' be mult. characters. Define the Jacobi sum

$$J(\chi,\chi') = \sum_{\substack{x,y\in E \\ x+y=1}} \chi(x)\chi'(y) = J(\chi',\chi) = \sum_{x\in E} \chi(x)\chi'(1-x)$$

Theorem If $p \equiv 1 \bmod 4$ is prime then $p = a^2+b^2$ for some $a,b \in \mathbb{Z}$.

There is a character χ of order 4 : $\chi(x) \in \mathbb{Q}[i]$ since $p \equiv 1 \bmod 4$,

$J(\chi) = a+bi$, $|J(\chi)|^2 = p = a^2+b^2$.