Finite Fields

Theorem The map

$$\{\text{finite fields}\} \longleftrightarrow \{p^k \mid p \in \mathbb{Z}_{>0}, p \text{ prime}, k \in \mathbb{Z}_{>0}\}$$

$$\mathbb{F} \longmapsto \mathrm{Card}(\mathbb{F})$$

$$\mathbb{F}_{p^k} \longleftarrow\!\shortmid\ p^k$$

is a bijection.

Examples $\mathbb{F}_2 = \{0,1\} = \mathbb{Z}/2\mathbb{Z}$,

$\mathbb{F}_3 = \{0,1,2\} = \mathbb{Z}/3\mathbb{Z}$,

$\mathbb{F}_4 \neq \mathbb{Z}/4\mathbb{Z}$ since $2 \cdot 2 = 0$ in $\mathbb{Z}/4\mathbb{Z}$

$\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z} = \{0,1,2,3,4\}$

$\mathbb{F}_6$ does not exist.

$\mathbb{F}_4 = \mathbb{F}_2[\xi] = \{a + b\xi \mid a, b \in \mathbb{F}_2\}$ with $\xi^2 + \xi + 1 = 0$.

So $\mathbb{F}_4 = \{0, 1, \xi, 1+\xi\}$ and $1+1=0$

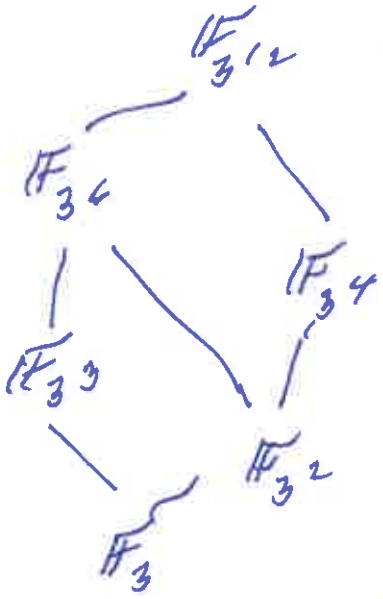
$\xi^2 = -\xi - 1 = 1 + \xi$, $\quad \xi(1+\xi) = \xi + \xi^2 = \xi + 1 + \xi = 1$

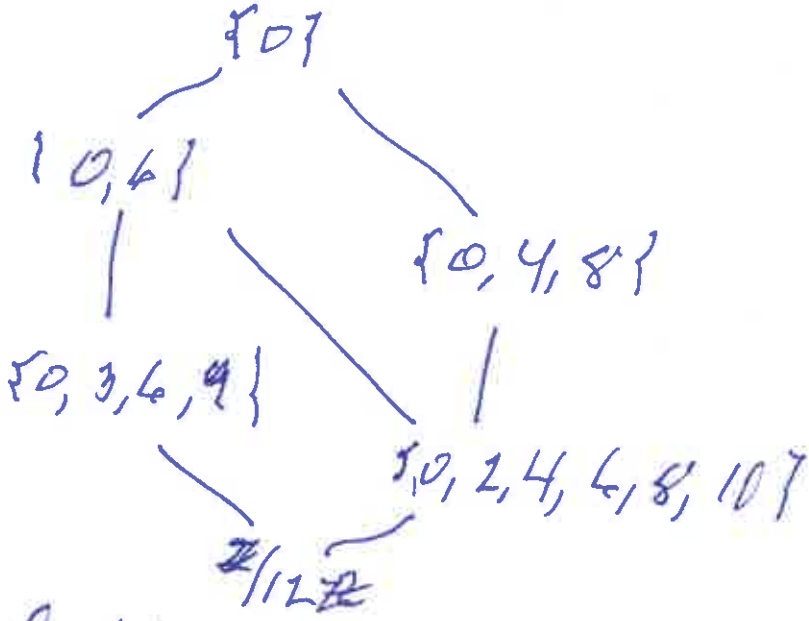
$(1+\xi)^2 = 1 + 2\xi + \xi^2 = 1 + (1+\xi) = \xi$.

So $\mathbb{F}_4^\times = \{1, \xi, \xi^2\} \cong \mathbb{Z}/3\mathbb{Z}$.

$\mathrm{Aut}_{\mathbb{F}_3}(\mathbb{F}_{3^{12}}) \cong \mathbb{Z}/12\mathbb{Z}$

$$\left\{\begin{array}{l}\text{fields } \mathbb{F} \text{ with} \\ \mathbb{F}_3 \subseteq \mathbb{F} \subseteq \mathbb{F}_{3^{12}}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{subgroups } H \\ \{0\} \subseteq H \subseteq \mathbb{Z}/12\mathbb{Z}\end{array}\right\}$$





Properties of Finite fields

(1) The algebraic closure of $\mathbb{F}_p$ is

$$\overline{\mathbb{F}}_p = \bigcup_{k \in \mathbb{Z}_{>0}} \mathbb{F}_{p^k}$$ (this is an infinite field)

(2) $$\mathbb{F}_{p^k} = \{\alpha \in \overline{\mathbb{F}}_p \mid \alpha^{p^k} = \alpha\}$$

$$= \{\alpha \in \overline{\mathbb{F}}_p \mid F^k(\alpha) = \alpha\} = \overline{\mathbb{F}}_p^{F^k}$$

where

$$F : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p, \quad \alpha \mapsto \alpha^p$$ and $$F^k : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p, \quad \alpha \mapsto \alpha^{p^k}.$$

(3) $\mathbb{F}_{p^n} \supseteq \mathbb{F}_{p^d}$ if d divides n.

Let $m \in \mathbb{Z}_{>0}$ such that $m d = n$. Then

$$\mathrm{Aut}_{\mathbb{F}_{p^d}}(\mathbb{F}_{p^n}) = \{1, F^d, F^{2d}, \ldots, F^{(m-1)d}\} \cong \mathbb{Z}/m\mathbb{Z}$$

Cyclotomic polynomials Let $n \in \mathbb{Z}_{>0}$

the set of primitive n^{th} roots of 1 in $\mathbb{C}$ is

$$\Pi_n = \{\omega \in \mathbb{C} \mid \omega^n = 1 \text{ and if } m \in \mathbb{Z}_{>0} \text{ and } m < n \text{ then } \omega^m \neq 1\}$$

the n^{th} cyclotomic polynomial is

$$\Phi_n(x) = \prod_{\alpha \in \Pi_n} (x - \alpha)$$

Examples

$\Pi_1 = \{1\}$ and $\Phi_1 = x - 1$

$\Pi_2 = \{-1\}$ and $\Phi_2 = x + 1 = \dfrac{x^2 - 1}{x - 1}$

$\Pi_3 = \{e^{2\pi i/3}, e^{2 \cdot 2\pi i/3}\}$ and $\Phi_3 = x^2 + x + 1 = \dfrac{x^3 - 1}{x - 1}$

$\Pi_4 = \{i, -i\}$ and $\Phi_4 = x^2 + 1 = \dfrac{x^4 - 1}{(x+1)(x-1)}$

Then

$$\Phi_n = \frac{x^n - 1}{\prod_{\substack{d \mid n \\ d \neq n}} \Phi_d} \quad \text{or} \quad \prod_{d \mid n} \Phi_d = x^n - 1.$$

The group of units of $\mathbb{Z}/n\mathbb{Z}$ is

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{ a \in \mathbb{Z}/n\mathbb{Z} \mid \text{there exists } b \in \mathbb{Z}/n\mathbb{Z} \text{ with } ba = 1 = ab \}$$

Proposition Let $n \in \mathbb{Z}_{>0}$ and $\omega = e^{2\pi i/n}$.
Then

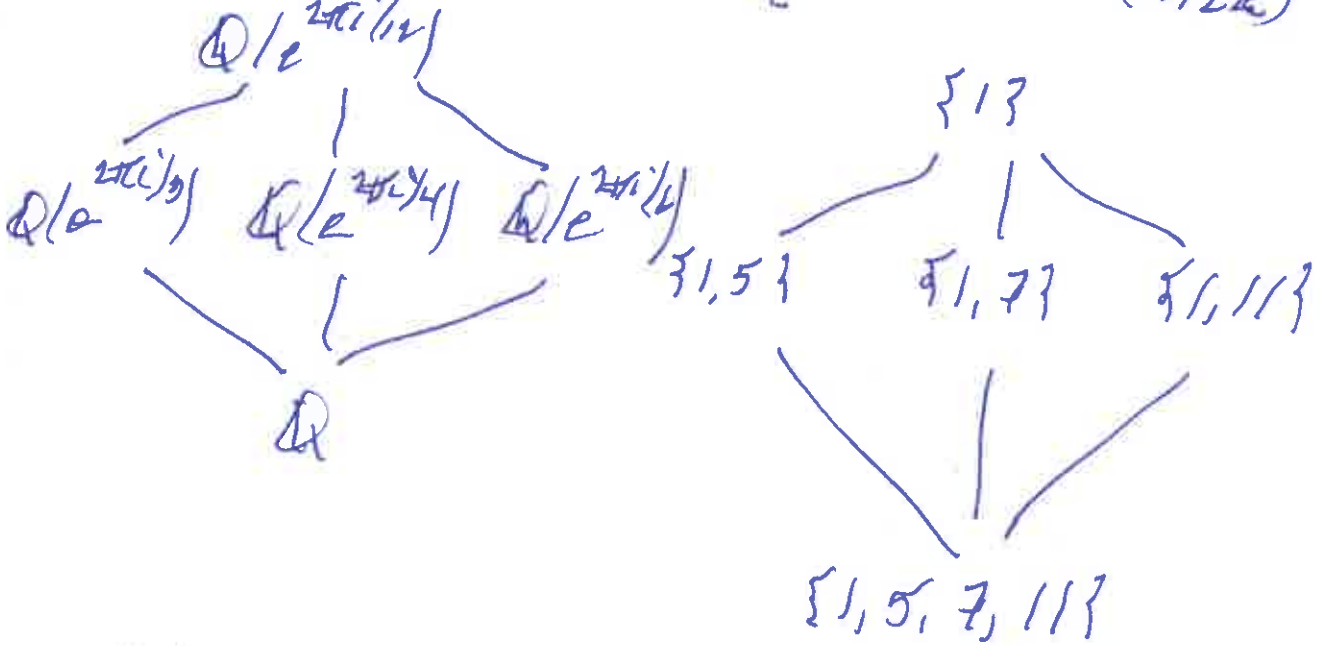
(a) $m_{\omega, \mathbb{Q}}(x) = \Phi_n(x)$

(b) $\deg(m_{\omega,\mathbb{Q}}(x)) = \dim_{\mathbb{Q}}(\mathbb{Q}(\omega)) = |\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega))|$

(c) $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

Example $n = 12$

$$\left\{ \begin{array}{c} \text{fields } F \text{ with} \\ \mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\omega) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subgroups } H \\ \{1\} \subseteq H \subseteq (\mathbb{Z}/12\mathbb{Z})^\times \end{array} \right\}$$



Note: In $\mathbb{Z}/12\mathbb{Z}$, $5^2 = 25 = 1$, $7^2 = 49 = 1$, and $11^2 = 121 = 1$.

Let $n \in \mathbb{Z}_{>0}$ and $d \in \mathbb{Z}_{>0}$ with $n\mathbb{Z} \subseteq d\mathbb{Z}$. Then

$$\mathbb{Q}(e^{2\pi i/n}) \supseteq \mathbb{Q}(e^{2\pi i/d}) \text{ and}$$

$$\mathrm{Gal}_{\mathbb{Q}(e^{2\pi i/d})}(\mathbb{Q}(e^{2\pi i/n})) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$$

where $m \in \mathbb{Z}_{>0}$ such that $md = n$.

Is this correct? Why?