

# CTNT 2024

Connecticut Summer School in Number Theory

## Class Field Theory

Christelle Vincent  
(University of Vermont)

First preliminary:  $\hat{\mathbb{Z}}$  Prüfer ring

Technically: projective limit

$$\varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$$

We need: If  $m|n$ , then there is

$$\varphi_{n,m} : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$$
$$a \mapsto a$$

$$\text{Gal}(L/\mathbb{Q})$$
$$\downarrow$$
$$\text{Gal}(K/\mathbb{Q})$$

"reduce more"

We need: If  $m|n$ , then there is

$$\varphi_{n,m}: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$$
$$a \mapsto a$$

"reduce more"

$$a \equiv b \pmod{n} \Leftrightarrow a = b + kn, k \in \mathbb{Z}$$

$$a \equiv b \pmod{m} \Leftrightarrow a = b + klm$$
$$l \in \mathbb{Z}$$

$$\mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}$$
$$1 \mapsto 1$$
$$7 \mapsto 1$$

We need: If  $m|n$ , then there is

$$\varphi_{n,m} : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$$
$$a \mapsto a$$

"reduce more"

$a \in \hat{\mathbb{Z}}$  is a sequence  $(a_2, a_3, a_4, a_5, a_6, \dots)$

$$a_n \in \mathbb{Z}/n\mathbb{Z}$$

whenever  $m|n$ ,  $\varphi_{n,m}(a_n) = a_m$

$$\mathbb{Z} \subseteq \hat{\mathbb{Z}}$$

$$a = 10 \in \mathbb{Z} \rightsquigarrow (0, 1, 2, 0, \overset{= a_6}{4}, 3, 2, 1, 0, 10, \dots)$$

$$(a_2, a_3, \underline{a_4}, \underline{a_5}, a_6, a_7, \underline{a_8}, \underline{a_9}, a_{10}, \dots)$$

Sun zi's Remainder Theorem

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$$
$$(a_2, a_3) \quad a_6$$

$$\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$$

Two facts

- $\mathbb{Z}$  is dense in  $\hat{\mathbb{Z}}$
- $n\hat{\mathbb{Z}}$   $n \in \mathbb{Z}$  are exactly the open subsets of  $\hat{\mathbb{Z}}$

## Preliminary 2: (Infinite) Galois theory

Definition:  $L/K$  is a field extension

This extension is Galois if it is

- algebraic: every  $\alpha \in L$  is the root of a polynomial in  $K[x]$ .  
 $\Rightarrow \alpha$  is a root of an irreducible poly  $m_{\alpha, K}(x) \in K[x]$
- normal: if  $f(x) \in K[x]$  is irreducible and it has a root in  $L$ , then all its roots

- normal: if  $f(x) \in K[x]$  is irreducible and it has a root in  $L$ , then all the roots of  $f$  are also in  $L$ .
- separable: the minimal polynomial of every  $\alpha \in L$  over  $K$  ( $m_{\alpha, K}$ ) has all distinct roots.

In this case  $\text{Aut}(L/K) = \text{Gal}(L/K)$

automorphisms of  $L$  that fix  $K$   
 $\sigma(\beta) = \beta \quad \forall \beta \in K$



When  $[L:K] < \infty$  then there is a bijection

subfields

closed  
subgroups

$$K \subseteq E \subseteq L$$

$$\text{Gal}(L/K) \supseteq H \supseteq 1$$

$$H = \text{Gal}(L/E)$$

$$E = L^H = \{l \in L : \sigma(l) = l, \sigma \in H\}$$

Of interest to us:

Base field  $k$

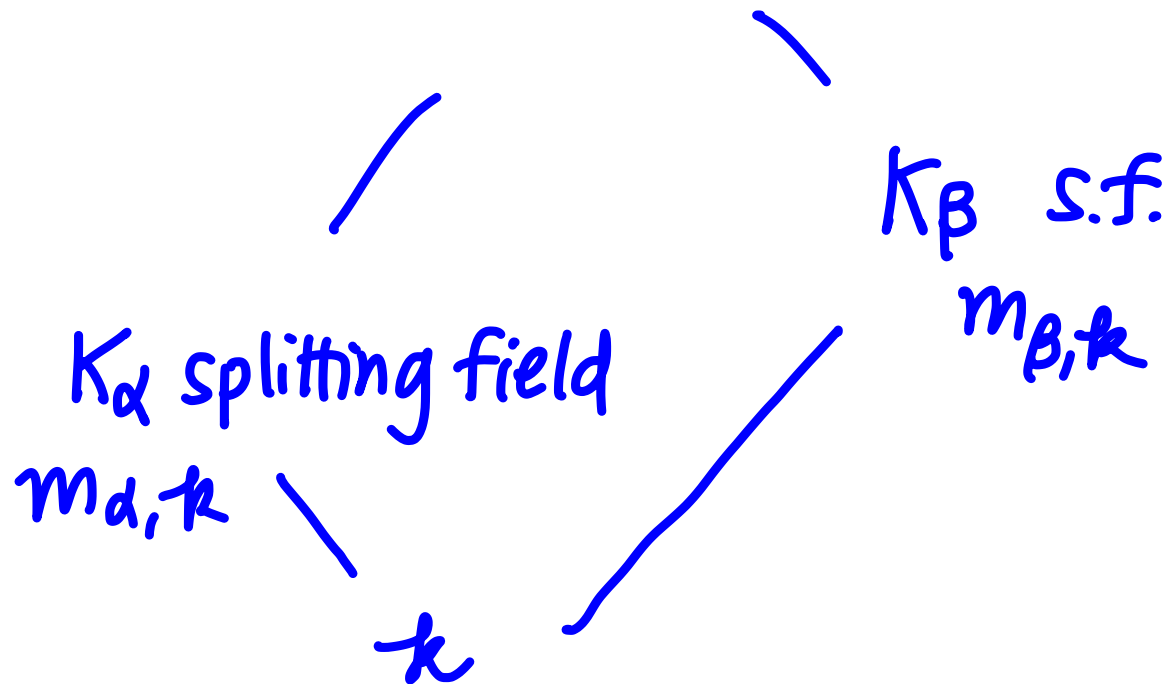
$\alpha \in \bar{k}$  separable closure

then 
$$\text{Gal}(\bar{k}/k) = \varprojlim_{\substack{K/k \\ \text{finite Galois}}} \text{Gal}(K/k)$$

$\alpha \in \bar{k}$  is algebraic over  $k$  with separable  $m_{\alpha, k}$

$$\text{Gal}(\bar{k}/k) = \varprojlim_{\substack{K/k \\ \text{finite Galois}}} \text{Gal}(K/k)$$

$d \in \bar{k}$  is algebraic over  $k$  with separable  $m_{d,k}$



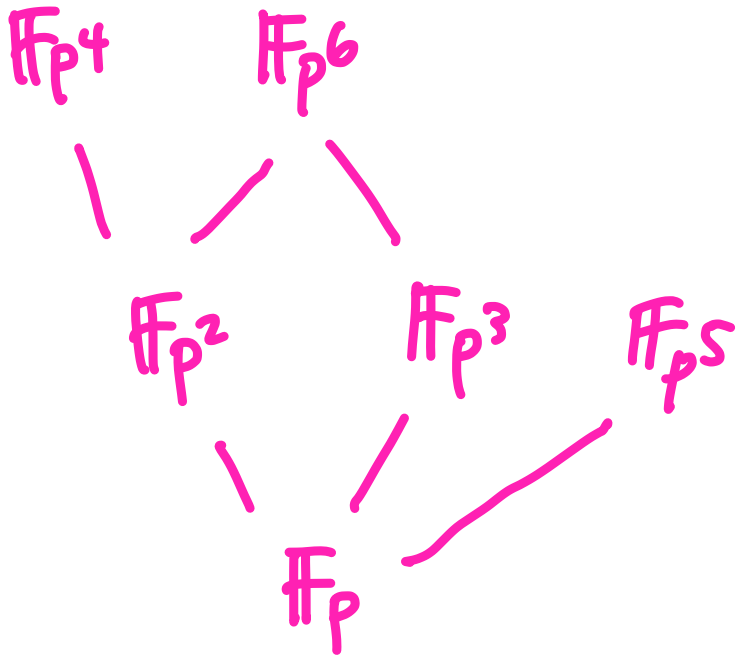
Example:  $k = \mathbb{F}_p$   $p$  prime

$$\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \quad \psi: x \mapsto x^p$$

$$\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^s} \\ \text{iff } r \mid s$$

$$\varprojlim_{\substack{K/\mathbb{F}_p \\ \text{finite}}} \text{Gal}(K/\mathbb{F}_p) = \varprojlim_n \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$$

$$= \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \hat{\mathbb{Z}}$$



$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$

$$\psi: x \mapsto x^p \mapsto 1$$

$$\varphi: x \mapsto x^p$$

$$\varphi \in \langle \varphi \rangle$$

For each  $n$ , write  $n = n' p^e$   $\gcd(p, n') = 1$

$$\text{define } x_n \equiv (n')^{-1} \pmod{p^e}$$

$$\text{define } a_n = n' x_n$$

$$\varphi \in \text{Gal}(\overline{\mathbb{F}_p} / \mathbb{F}_p) \quad (\varphi_2, \varphi_3, \varphi_4, \dots)$$

$$\varphi_n = \varphi^{a_n}$$