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 $m \mid n$, then there is

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

"reduce more"

$$\begin{array}{c} \mathrm{Gal}(L/\mathbb{Q}) \\ \downarrow \\ \mathrm{Gal}(K/\mathbb{Q}) \end{array}$$

We need: If $m \mid n$, then there is

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

"reduce more"

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

$$a \equiv b \bmod m \Leftarrow a = b + klm$$
$$l \in \mathbb{Z}$$

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

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

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

"reduce more"

$(\sigma_K \qquad \sigma_L$

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

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

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

$\mathbb{Z} \subsetneq \hat{\mathbb{Z}}$

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

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

Sun Zi's Remainder Theorem

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$$

$$(a_2, a_3) \qquad\qquad a_6$$

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

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 <u>Galois</u> if it is

- algebraic: every $\alpha \in L$ is the root of a polynomial in $K[x]$.
  $\Rightarrow$ α 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 $\mathrm{Aut}(L/K) = \mathrm{Gal}(L/K)$

automorphisms of L that fix K

$\sigma(\beta) = \beta \quad \forall \beta \in K$

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

subfields | closed subgroups

$K \subseteq E \subseteq L$ | $\mathrm{Gal}(L/K) \supseteq H \supseteq 1$

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

$$E = L^H = \{\ell \in L : \sigma(\ell) = \ell.\ \sigma \in H\}$$

Of interest to us:

Base field k

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

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

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

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

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

$$\begin{tikzcd}
 & \bar{k} \arrow[dl, dash] \arrow[dr, dash] & \\
K_\alpha \text{ splitting field } m_{\alpha,k} \arrow[dr, dash] & & K_\beta \text{ s.f. } m_{\beta,k} \arrow[dl, dash] \\
 & k &
\end{tikzcd}$$

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

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

$$\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \qquad \varphi : x \mapsto x^p$$

$$\| $$

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

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

$$\varphi \mapsto 1$$

$$\begin{tikzcd}
\mathbb{F}_{p^4} \arrow[dr, dash] & & \mathbb{F}_{p^6} \arrow[dl, dash] \arrow[dr, dash] & & \\
& \mathbb{F}_{p^2} \arrow[dr, dash] & & \mathbb{F}_{p^3} \arrow[dl, dash] & \mathbb{F}_{p^5} \arrow[dll, dash] \\
& & \mathbb{F}_p & &
\end{tikzcd}$$

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

$$\varphi : x \mapsto x^p \quad \mapsto \quad 1$$

$\varphi : x \mapsto x^p$

$\psi \notin \langle \varphi \rangle$

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

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

define $a_n = n' x_n$

$\psi \in Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ $(\psi_2, \psi_3, \psi_4, \ldots)$

$\psi_n = \varphi^{a_n}$