CTNT 2024

Connecticut Summer School in Number Theory

Class Field Theory

Christelle Vincent
(University of Vermont)

Last time

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

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

the Frobenius

① Every finite $K/\mathbb{F}_p$ $\quad (K = \mathbb{F}_{p^n})$

has a Frobenius!

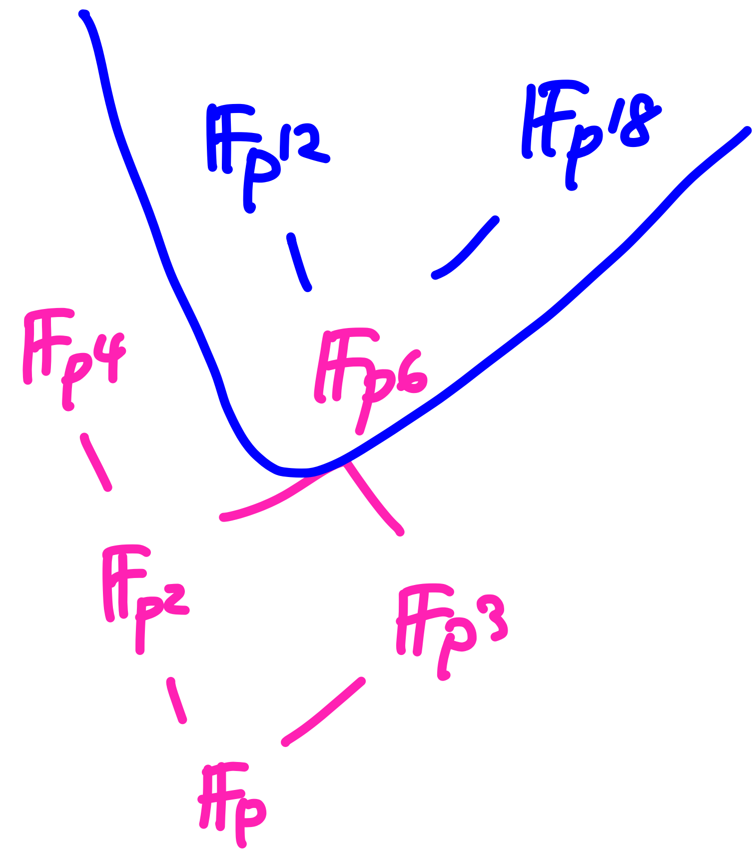
if $q = p^n$ $\quad \mathrm{Gal}(\overline{\mathbb{F}}_p/K) = \mathrm{Gal}(\overline{K}/K)$

① Every finite $K/\mathbb{F}_p$ $\quad (K=\mathbb{F}_{p^n})$

has a Frobenius!

if $q=p^n$ $\quad \mathrm{Gal}(\overline{\mathbb{F}_p}/K)=\mathrm{Gal}(\overline{K}/K)$

$$\varphi_K: x\mapsto x^q$$



$$\mathrm{Gal}(\overline{K}/K)\cong\hat{\mathbb{Z}}$$

$$\varphi_K: x\mapsto x^q \;\mapsfrom\; 1$$

② Let $K/\mathbb{F}_p$ be finite, $\sigma \in \mathrm{Gal}(K/\mathbb{F}_p)$

then σ can be a Frobenius too!

$$\begin{array}{c} K \\ | \\ \mathbb{F}_p \end{array}$$

$\mathrm{Gal}(K/\mathbb{F}_p) = \langle \varphi|_K \rangle$

so $\sigma = \varphi|_K^{\,n}$ n pos. integer

extend σ to $\tilde{\sigma} \in \mathrm{Gal}(\bar{K}/\mathbb{F}_p)$

take $\tilde{\sigma} = \varphi^n$

Let Σ be the fixed field of $\tilde{\sigma}$, then $\tilde{\sigma} = \varphi_\Sigma$

Example

$$\begin{tikzcd}[column sep=small]
& \overline{\mathbb{F}}_p \arrow[dl, dash] \arrow[d, dash] \\
K = \mathbb{F}_{p^6} \arrow[ddr, dash] & \\
& \mathbb{F}_{p^4} \arrow[d, dash] \\
& \mathbb{F}_p
\end{tikzcd}$$

$\mathrm{Gal}(K/\mathbb{F}_p) = \langle \varphi|_K \rangle$

$\varphi : x \mapsto x^p$

$\sigma = \varphi|_K^4 : \; x \mapsto x^{p^4}$

take $\tilde{\sigma} : x \mapsto x^{p^4} \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$

the fixed field of $\tilde{\sigma}$ is

$\mathbb{F}_{p^4}$ and $\tilde{\sigma} = \varphi_{\mathbb{F}_{p^4}}$

Class field theory for $k = \mathbb{Q}_p$

base field

Facts about finite extensions $K/\mathbb{Q}_p$

- K is also a complete field with a discrete valuation
- $\mathcal{O}_K$ integral closure of $\mathbb{Z}_p$ in K is a DVR: it has a unique prime ideal $\mathfrak{p} = (\pi_K)$

- $\mathcal{O}_K$ integral closure of $\mathbb{Z}_p$ in K is a DVR: it has a unique prime ideal $\mathfrak{p} = (\pi_K)$

$$p\mathcal{O}_K = \mathfrak{p}^{e_K}$$

$$\Big[\underbrace{\mathcal{O}_K/\mathfrak{p}}_{\text{finite field}} : \underbrace{\mathbb{F}_p}_{\mathbb{Z}_p/(p)}\Big] = f_K$$

Fact

$$[K:\mathbb{Q}_p] = e_K \cdot f_K$$

If $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$

then $\sigma(\mathfrak{p}) = \mathfrak{p}$ so every $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$

descends to $\mathcal{O}_K/\mathfrak{p}$

$$\begin{aligned} \mathrm{Gal}(K/\mathbb{Q}_p) &\longrightarrow \mathrm{Gal}(\mathbb{F}_{p^{f_K}}/\mathbb{F}_p) \cong \mathbb{Z}/f_K\mathbb{Z} \\ \sigma \quad &\qquad\quad \sigma \bmod \mathfrak{p} \end{aligned}$$

if $e_K = 1$ $\quad p\mathcal{O}_K = \mathfrak{p}$ unramified $\quad f_K = [K:\mathbb{Q}_p]$

$$\begin{aligned} \mathrm{Gal}(K/\mathbb{Q}_p) &\cong \mathrm{Gal}(\mathbb{F}_{p^{f_K}}/\mathbb{F}_p) = \mathbb{Z}/f_K\mathbb{Z} \\ \varphi \quad &\longmapsfrom \quad \varphi \quad \longmapsfrom \quad 1 \end{aligned}$$

Fact: $\mathbb{Q}_p$ has a maximal unramified extension, denoted $\widetilde{\mathbb{Q}_p} \subseteq \overline{\mathbb{Q}_p}$

and

$$\begin{array}{ccccc} \mathrm{Gal}(\widetilde{\mathbb{Q}_p}/\mathbb{Q}_p) & \cong & \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) & \cong & \hat{\mathbb{Z}} \\ \varphi & \leftarrow\!\shortmid & x \mapsto x^p & \leftarrow\!\shortmid & 1 \end{array}$$

$$\sigma \longmapsto n \in \mathbb{Z}$$

the Frobenius

tells me $\sigma = \varphi^n$

Also

$$d: \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \twoheadrightarrow \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \hat{\mathbb{Z}}$$

$$\sigma \qquad \left[x \mapsto x^p \leftarrow\!\shortmid 1 \right]$$

$$\sigma \longmapsto n \in \mathbb{Z}$$

$$\begin{tikzcd}
\boxed{d : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \twoheadrightarrow \hat{\mathbb{Z}}} \arrow[d] & \\
\mathrm{Gal}(\widetilde{\mathbb{Q}}_p/\mathbb{Q}_p) \arrow[r, "\sim"] & \hat{\mathbb{Z}}
\end{tikzcd}$$

$$I = \mathrm{Ker}\, d = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\widetilde{\mathbb{Q}}_p)$$

Let $K/\mathbb{Q}_p$ finite extension

$\tilde{K} = K\tilde{\mathbb{Q}}_p$ maximal unramified extension of K

$$d : \mathrm{Gal}(\bar{K}/K) \xrightarrow{\text{not surjective}} \hat{\mathbb{Z}}$$

$$\|$$

$$\mathrm{Gal}(\bar{\mathbb{Q}}_p/K) \leq \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$$

$$x \mapsto x^{p^n} \longrightarrow n$$

$$\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_{p^n}) \longrightarrow \hat{\mathbb{Z}} \ni 1$$

$$\leq$$

$$\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) \ni x \mapsto x^p$$

Let $f_K = [\hat{\mathbb{Z}} : d(\mathrm{Gal}(\bar{K}/K))]$
$= [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$

$$d_K = \frac{1}{f_K} d : \mathrm{Gal}(\bar{K}/K) \twoheadrightarrow \hat{\mathbb{Z}}$$

We say $\sigma \in \mathrm{Gal}(\bar{K}/K)$ is "a" Frobenius for K if $d_K(\sigma) = 1$

$d_K = \dfrac{1}{f_K}\, d : \mathrm{Gal}(\bar{K}/K) \twoheadrightarrow \hat{\mathbb{Z}}$

We say $\sigma \in \mathrm{Gal}(\bar{K}/K)$ is "a" Frobenius for K if $d_K(\sigma) = 1$ notation φ_K

Every $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$ is a Frobenius somewhere

$$\begin{tikzcd}[column sep=small]
 & \tilde{K} \arrow[ddl, dash, "\tilde{\sigma}"] \\
K \arrow[ur, dash] \arrow[d, dash, "\sigma"'] & \\
\mathbb{Q}_p &
\end{tikzcd}$$

$d(\tilde{\sigma}) = n = f_\Sigma$

Let Σ be the fixed field of $\tilde{\sigma}$

then $\tilde{\sigma} = \varphi_\Sigma$

CTNT 2024

Connecticut Summer School in Number Theory

... That's all for now ...