LOCAL GALOIS MODULE THEORY AND RAMIFICATION: AN OVERWIEV

1) p-adic fields

· Fröhlich, Taylor, "Algebraic number theory"

2) Ramification theory

· Serre, "Local fields"

3) Local Galois module theory

· Thomas, "On the Galois module structure of extensions of local fields"

· Johnston, "Notes on Galois modules"

· Ferri, Stefanello, "Galois and Hopf Galois"

P: prime number

1) P-ADIC FIELDS

DEF: The p-ADIC VALUATION on $\mathbb{Q}$ is

$$v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$$
$$0 \longmapsto \infty$$
$$0 \neq \frac{a}{b} = p^v \frac{c}{d} \longmapsto v \quad \text{where } (c,p) = (d,p) = 1.$$

LEMMA: v_p is a DISCRETE VALUATION

1) $v_p(a) = \infty \iff a = 0$
2) $v_p(ab) = v_p(a) + v_p(b)$
3) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$

FACT: v_p induces a Topology on $\mathbb{Q}$

DEF: The FIELD of P-ADIC NUMBERS $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ WRT this Topology.

$$\mathbb{Q}_p = \left\{ \sum_{n=i}^{+\infty} a_n p^n \;\middle|\; a_n \in \{0, \dots, p-1\} \right\}$$

RK: i can be negative

DEF: A P-ADIC FIELD K is a finite extension of $\mathbb{Q}_p$

FACTS: 1) K is complete WRT the topology given by a discrete valuation $v_K : K \longrightarrow \mathbb{Z} \cup \{\infty\}$

FOR $\mathbb{Q}_p$: $v_{\mathbb{Q}_p}\left(\sum a_n p^n\right) = \min\{n \mid a_n \neq 0\}$.

2) The VALUATION RING of K is

$$\mathcal{O}_K = \{ x \in K \mid v_K(x) \geq 0 \}$$

$\mathcal{O}_K$ is DEDEKIND DOMAIN + LOCAL RING (DVR $\Rightarrow$ PID)

FOR $\mathbb{Q}_p$: $\mathcal{O}_{\mathbb{Q}_p} = \mathbb{Z}_p = \{ \sum_{n \geq 0} a_n p^n \}$ RING OF P-ADIC INTEGERS

3) The PRIME of K is the unique maximal ideal

$$\mathfrak{p}_K = \{ x \in K \mid v_K(x) > 0 \}$$

$\mathfrak{p}_K = \pi_K \mathcal{O}_K$, where $v_K(\pi_K) = 1$ (UNIFORMISER)

FOR $\mathbb{Q}_p$: $\pi_{\mathbb{Q}_p} = p$, $\mathfrak{p}_{\mathbb{Q}_p} = p\mathbb{Z}_p$

4) The RESIDUE FIELD of K is $\mathcal{O}_K / \mathfrak{p}_K = k_K$.

$\Rightarrow |k_K|$ is a power of p.

FOR $\mathbb{Q}_p$: $\mathbb{Z}_p / p\mathbb{Z} \cong \mathbb{Z} / p\mathbb{Z} = \mathbb{F}_p$.

2. RAMIFICATION THEORY

RECALL: K p-adic field, $v_K : K \to \mathbb{Z} \cup \{\infty\}$

- $\mathcal{O}_K = \{x \in K \mid v_K(x) \geq 0\}$
- $P_K = \{x \in K \mid v_K(x) > 0\} = \pi_K \mathcal{O}_K$, where $v_K(\pi_K) = 1$.
- $k_K = \mathcal{O}_K / P_K$

Let L/K be an extension of p-adic fields.

1) $k_K = \frac{\mathcal{O}_K}{P_K} \hookrightarrow \frac{\mathcal{O}_L}{P_L} = k_L$, $[k_L : k_K] = f_{L/K}$

INERTIA DEGREE $\to$ $f_{L/K}$

2) $P_K \mathcal{O}_L = P_L^{e_{L/K}}$ $\leftarrow$ RAMIFICATION INDEX

($e_{L/K} = v_L(\pi_K)$)

FACT: $[L:K] = e_{L/K} \cdot f_{L/K}$

DEF: L/K is

- UNRAMIFIED if $e_{L/K} = 1 \iff f_{L/K} = [L:K]$.
- TOTALLY RAMIFIED if $e_{L/K} = [L:K] \iff f_{L/K} = 1$.
- TAMELY RAMIFIED if $p \nmid e_{L/K}$ (otherwise, WILDLY RAMIFIED)

Now fix a Galois extension L/K of p-adic fields, $G = Gal(L/K)$

DEF: $\forall i \geq -1$, the ith-RAMIFICATION GROUP is

$$G_i = \{\sigma \in G \mid \sigma(x) - x \in \mathfrak{P}_L^{i+1} \quad \forall x \in \mathcal{O}_L\}$$

FACTS: $\cdot$ $G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m = \{1\}$, $G_i \trianglelefteq G$.

$\cdot$ $G_0 = \{\sigma \in G \mid \sigma(x) - x \in \mathfrak{P}_L \ \forall x \in \mathcal{O}_L\}$ INERTIA SUBGROUP.
$|G_0| = e_{L/K} \Rightarrow$ L/K UNRAMIFIED $\Leftrightarrow$ $G_0 = \{1\}$

$\cdot$ G_1 is a Sylow p-subgroup of G_0. In particular,
L/K TAMELY RAMIFIED $\Leftrightarrow$ $p \nmid e_{L/K} \Leftrightarrow$ $G_1 = \{1\}$

DEF: L/K is WEAKLY RAMIFIED if $G_2 = \{1\}$

DEF: a RAMIFICATION JUMP is $t \in \mathbb{Z}$ s.t. $G_t \neq G_{t+1}$

DEF: The DIFFERENT of L/K is the ideal of $\mathcal{O}_L$:

$$\mathcal{D}_{L/K}^{-1} = \{x \in L \mid Tr_{L/K}(xy) \in \mathcal{O}_K \quad \forall y \in \mathcal{O}_L\}$$

(where $Tr_{L/K}(xy) = \sum_{\sigma \in G} \sigma(xy)$)

FACT: $\mathcal{D}_{L/K}$ contains important arithmetic information

PROP (HILBERT'S FORMULA): $\mathcal{D}_{L/K} = \mathfrak{P}_L^{v}$

$$v = \sum_{i=0}^{+\infty} (|G_i| - 1)$$

EXA: Assume that L/K is

- TOTALLY RAMIFIED ($e_{L/K} = [L:K] \Leftrightarrow G_0 = G$)
- p-extension ($G_1 = G_0 = G$)
- weakly ramified ($G_2 = 1$)

$$\Rightarrow \quad \mathcal{D}_{L/K} = \mathfrak{P}_L^{2|G|-2}$$

3. LOCAL GALOIS MODULE THEORY

Let R be a ring, and let H be a finite group.

DEF: The GROUP ALGEBRA is

$$R[H] = \left\{ \sum_{\sigma \in H} r_\sigma \sigma \mid r_\sigma \in R \right\}$$

1) $R[H]$ is a free (left) R-module with basis H.

2) $R[H]$ is an R-algebra (MODULE + RING + COMPATIBILITY):

$$(r_\sigma \sigma) \cdot (r_\tau \tau) = \underbrace{r_\sigma r_\tau}_{\in R} \underbrace{\sigma\tau}_{\in H}$$

RECALL: L/K is a Galois extension of p-adic fields, $G = Gal(L/K)$

EXA: $K[G]$, $\mathcal{O}_K[G]$ are examples.

L is a $K[G]$-module, $\mathcal{O}_L$ is an $\mathcal{O}_K[G]$-module.

$$\left(\sum K_\sigma \sigma\right) \cdot x = \sum K_\sigma \sigma(x)$$

THM (NORMAL BASIS): L is a free $K[G]$-module (of rank one)
This means that (equivalently):

1) $L \cong K[G]$ as $K[G]$-modules ($L = K[G] \cdot \alpha$)

2) L/K admits a NORMAL BASIS:

$\{\sigma(\alpha) \mid \sigma \in G\}$ is a K-basis of L

QUESTION: Is also $\mathcal{O}_L$ a free $\mathcal{O}_K[G]$-module?

Equivalently, does L/K admit a NORMAL INTEGRAL BASIS (NIB)?

$\{\sigma(\alpha) \mid \sigma \in G\}$ $\mathcal{O}_K$-basis of $\mathcal{O}_L$

ANSWER: not true in general!

THM (NOETHER, ULLOM, KAWAMOTO): The following are equivalent:

a) $\mathcal{O}_L$ is free over $\mathcal{O}_K[G]$ (of rank one) $\Leftrightarrow$ L/K has NIB

b) L/K is tamely ramified ($p \nmid e_{L/K} \Leftrightarrow G_1 = \{1\}$)

PROOF: ($\Rightarrow$) "easy"

($\Leftarrow$) more difficult.

We show just one part: if L/K is UNRAMIFIED, then $\mathcal{O}_L$ is free over $\mathcal{O}_K[G]$.

$$\text{UNRAM.} \Rightarrow \begin{cases} P_K \mathcal{O}_L = P_L \\ [k_L : k_K] = [L:K],\ G = Gal(L/K) \cong Gal(k_L/k_K) \end{cases}$$

BY NBT: $k_L = k_K[G] \cdot \bar{\alpha}$, $\quad \bar{\alpha} = \alpha + P_L,\ \alpha \in \mathcal{O}_L$

$$k_L = \frac{\mathcal{O}_L}{P_L}, \quad k_K = \frac{\mathcal{O}_K}{P_K}$$

$$\mathcal{O}_L = \mathcal{O}_K[G] \cdot \alpha + P_L = \mathcal{O}_K[G] \cdot \alpha + P_K \mathcal{O}_L$$

NAKAYAMA

$\Rightarrow$ $\mathcal{O}_L = \mathcal{O}_K[G] \cdot \alpha$, $\mathcal{O}_L$ is free over $\mathcal{O}_K[G]$

QUESTION: What if L/K is wildly ramified?

DEF (LEOPOLDT): The ASSOCIATED ORDER of $\mathcal{O}_L$ in $K[G]$ is

$$A_{L/K} = \{\lambda \in K[G] \mid \lambda \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}$$

FACTS: 1) $A_{L/K}$ is an $\mathcal{O}_K$-subalgebra of $K[G]$.

$\mathcal{O}_K[G] \subseteq A_{L/K}$, "=" $\Leftrightarrow$ L/K tamely ramified

2) $\mathcal{O}_L$ is a $A_{L/K}$-module

3) If $\mathcal{O}_L$ is free of rank one over M, where M is an $\mathcal{O}_K$-subalgebra of $K[G]$, then $M = A_{L/K}$

QUESTION: Is $\mathcal{O}_L$ free (of rank one) over $A_{L/K}$?

STRATEGIES: Assumptions on

- the group structure of G
- ramification of L/K

GROUP STRUCTURE:

$\mathcal{O}_L$ is free over $A_{L/K} = \{\lambda \in K[G] \mid \lambda \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}$ if

1) G is dihedral of order $2p$ (Bergé, 1972)

2) G is $\cong$ to a suitable $C_p \rtimes C_m$ (Jaulent, 1981)

3) $Gal(L/\mathbb{Q}_p)$ is abelian ($\Rightarrow G$ abelian) (Lettl, 1998)

and more...

RAMIFICATION:

$\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K} = \{\lambda \in K[G] \mid \lambda \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}$ if

1) L/K is tamely ramified ($\mathfrak{A}_{L/K} = \mathcal{O}_K[G]$) (Ullom, 1970)

2) $|G| = p$, $t = t_0 p + a$ ($a \in \{0, \dots, p-1\}$) unique ramification jump,
   - $t \equiv 0 \mod p$
   - or $t < \frac{p v_K(p)}{p-1}$ and $a \mid p-1$

   (BERTRANDIAS – FERTON, 1972)

...

3) L/K is WEAKLY RAMIFIED ($G_2 = 1$) (JOHNSTON, 2015)
   ↳ KEY FACT: if L/K is totally and weakly ramified p-exten.

$$D_{L/K} = P_L^{2|G|-2} \Rightarrow Tr_{L/K}(P_L) = P_K^2 \Rightarrow P_L = \mathcal{O}_K[G] \cdot \pi_L \Rightarrow \dots$$

and more ... Thomas's survey of 2010 has 162 bibliography entries!

QUESTION: What if $\mathcal{O}_L$ is not free over $\mathfrak{A}_{L/K}$?

We can try to use HOPF-GALOIS THEORY

"CLASSICAL" GALOIS STRUCTURE	HOPF-GALOIS STRUCTURE
L/K, $G = Gal(L/K)$	L/K, $G = Gal(L/K)$
$K[G]$	H (K-HOPF ALGEBRA)
$K[G]$ acts on L	H acts on L (as $K[G]$)
$\mathfrak{A}_{L/K} = \{\lambda \in K[G] \mid \lambda \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}$	$\mathfrak{A}_H = \{h \in H \mid h \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}$
Q: Is $\mathcal{O}_L$ free over $\mathfrak{A}_{L/K}$?	Q: Is $\mathcal{O}_L$ free over $\mathfrak{A}_H$?

FACT (BYOTT): There are extensions L/K s.t.

a) $\mathcal{O}_L$ is not free over $\mathfrak{A}_{L/K}$

b) $\mathcal{O}_L$ is free over $\mathfrak{A}_H$