Local Galois Module Theory in Characteristic p
- Maria Marklove, Omaha, NE, May 2013.

Let K be a local field, complete with respect to a discrete valuation

$$v_K : K \to \mathbb{Z} \cup \{\infty\}.$$

Then K has:

- $\mathfrak{O}_K = \{x \in K : v_K(x) \geq 0\}$
- $\mathfrak{P}_K = \{x \in K : v_K(x) > 0\}$
- $k = O_K/\mathfrak{P}_K$
- Let L be a finite Galois extension of K and let $G = Gal(L/K)$.
- k perfect, char$(k) = p > 0$. Two cases:
- char$(K) = p$,
- char$(K) = 0$,

Aim: To study $\mathfrak{O}_L$ as an $\mathfrak{O}_K[G]$-module.

- Noether: $\mathfrak{O}_L$ is (locally) free over $\mathfrak{O}_K[G] \Leftrightarrow L/K$ is tame.
- Therefore in the wildly ramified case: $\mathfrak{O}_L$ is not locally free over $\mathfrak{O}_K[G]$.
- Can we enlarge $\mathfrak{O}_K[G]$, in order to obtain something in which $\mathfrak{O}_L$ is free over?

This motivates the definition of the associated order:

$$\mathcal{A}_{L/K}(\mathfrak{O}_L) = \{\alpha \in K[G] : \alpha\mathfrak{O}_L \subseteq \mathfrak{O}_L\}.$$

Some results (what we already know):

Char$(K) = 0$, degree p extension case: Betrandias', Ferton (1970s): $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}(\mathfrak{O}_L)$ iff $s \mid (p-1)$ where $b = q_0p + s$ $(1 \leq s \leq p-1)$ is the ramification number satisfying $b < \frac{ep}{p-1} - 1$.

Ferton: Necessary and sufficient conditions for $\mathfrak{P}_L^h$ (some $h \in \mathbb{Z}$) to be free over $\mathfrak{A}_{L/K}(\mathfrak{P}_L^h)$. These will be looked at in detail later.

Char$(K) = p$ degree p extensions case:

Aiba and Lettl: $\mathfrak{O}_L$ is free over $A_{L/K}$ iff $s|(p-1)$ where $b = q_0p + s$ $(1 \leq s \leq p-1)$ is the ramification number. Re-interpreted by Bart de Smit and Lara Thomas (dsT07) in a more algebraic way. Let $\mathfrak{m}$ be the (unique) maximal ideal of $\mathcal{A}_{L/K}(\mathfrak{O}_L)$. Then define the embedding dimension as:

$$edim(A_{L/K}(O_L)) := \dim_k(\mathfrak{m}/\mathfrak{m}^2)$$

then $\mathfrak{O}_L$ is free over $A_{L/K}(\mathfrak{O}_L)$ iff $edim(A_{L/K}(\mathfrak{O}_L)) \leq 3$.

Theorem 1. *(dsT07) Let K be a local field with char$(K) = p$, and let L/K be a totally ramified cyclic extension of degree p. Let $b = q_0p + s$ be the unique ramification number of L/K, with $1 \leq s \leq p-1$. Let d be the minimal number of $\mathcal{A}_{L/K}$-generators of $\mathfrak{O}_L$. Then $d = 1$ if and only if $\mathfrak{O}_L$ is free over $\mathcal{A}_{L/K}$ and:*

1. *if $s = p-1$ then $d = 1$ and edim$(\mathcal{A}_{L/K}) = 2$;*
2. *if $s < p-1$ then edim$(\mathcal{A}_{L/K}) = 2d+1$ and $d = \sum_{i<n, iodd} b_i$, where the b_i are the unique integers given by the continued fraction expansion:*

$$\frac{-s}{p} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{\ddots \, \cfrac{\ddots}{b_{n-1} + \frac{1}{b_n}}}}$$

where $b_1, \ldots, b_n \geq 1$ and $b_n \geq 2$.

In particular, $\mathfrak{O}_L$ is free over its associated order if and only if $s \mid (p-1)$.

Question: Given $h \in \mathbb{Z}$, when is $\mathfrak{P}_L^h$ free over

$$A_{L/K}(\mathfrak{P}_L^h) = \{\alpha \in K[G] : \alpha \mathfrak{P}_L^h \subseteq \mathfrak{P}_L^h\}$$

(for the degree p char$(K) = p$ case)?

Utilise dst07:

- Let $d =$ minimal number of $A_{L/K}$-module generators of O_L

and define:

$$\begin{aligned}
a_j &= \left\lceil \frac{js}{p} \right\rceil, \qquad \epsilon_j = a_j - a_{j-1} \\
m_n &= \inf\{\epsilon_{i+j} + \ldots + \epsilon_{i+n} : 0 \leq i \leq p-n\}, \ m_0 = 0 \\
D &= \{i : 0 < i < p : a_j + m_{i-j} < a_i \ \forall \ j : \ 0 < j < i\} \\
E &= \{i : 0 \leq i < p : m_j + m_{i-j} < m_i \ \forall \ j : \ 0 < j < i\}
\end{aligned}$$

Theorem (dST07):

- $d = |D|$,
- edim$(A_{L/K}(\mathfrak{O}_L)) = |E|$

It turns out we can add a h dependency on these sequences in order to obtain the equivalent conditions for $\mathfrak{P}_L^h$. For some $h \in \mathbb{Z}$ define:

$$\begin{aligned}
a_j^{(h)} &= \left\lceil \frac{h+js}{p} \right\rceil, \qquad \epsilon_j^{(h)} = a_j^{(h)} - a_{j-1}^{(h)} \\
m_n^{(h)} &= \inf\{\epsilon_{i+j}^{(h)} + \ldots + \epsilon_{i+n}^{(h)} : 0 \leq i \leq p-n\}, \ m_0^{(h)} = 0 \\
D^{(h)} &= \{i : 0 \leq i < p : a_i^{(h)} + m_{j-i}^{(h)} < a_j^{(h)} \ \forall \ j : \ i < j < p\} \\
E^{(h)} &= \{i : 0 \leq i < p : m_j^{(h)} + m_{i-j}^{(h)} < m_i^{(h)} \ \forall \ j : \ 0 < j < i\}
\end{aligned}$$

Note that 'E' has stayed the same but 'D' has changed defintion slightly. Proposition:

- $d = |D^{(h)}|$,
- edim$(A_{L/K}(\mathfrak{P}_L^h)) = |E^{(h)}|$

Byott & Elder (preprint): Define, WLOG, for $s-p+1 \leq h \leq s$,

$$\begin{aligned} d(j) &= \left\lfloor \frac{(j+1)s-h}{p} \right\rfloor \\ w(j) &= \min\{d(j+i)-d(i) \ \forall\ 0 \leq i \leq p-1-j\} \\ \mathcal{D} &= \{u : d(u) > d(u-j)+w(j) \ \forall\ 0 < j \leq u\} \\ \mathcal{E} &= \{u : w(u) > w(u-j)+w(j) \ \forall\ 0 < j < u\} \end{aligned}$$

Proposition 2. *$\mathcal{D} = D^{(h)}$ and $\mathcal{E} = E^{(h)}$*

Notation: Let $\frac{s}{p} = [q_0; q_1, \ldots, q_n]$ denote the continued fraction expansion of $\frac{s}{p}$.

Example 3. *Let $\frac{s}{p} = \frac{5}{13} = [0; 2, 1, 1, 2]$, also let $h = s$ and $0 \leq j \leq p-1$ so that $d(j) = \left\lfloor \frac{(j+1)s-h}{p} \right\rfloor = \left\lfloor \frac{js}{p} \right\rfloor$.*

j	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
$d(j)$	*0*	*0*	*0*	*1*	*1*	*1*	*2*	*2*	*3*	*3*	*3*	*4*	*4*
$w(j)$	*0*	*0*	*0*	*1*	*1*	*1*	*2*	*2*	*3*	*3*	*3*	*4*	*4*

$\mathcal{D} = \{0\}$ and $\mathcal{E} = \{0, 1, 3, 8\}$.

Note how we can describe these d's (and w's) in terms of 'blocks' of length 2 and of length 3 (horizontally). If we call the blocks of length 2 Short (S) and the blocks of length 3 Long (L) then we can describe the $\{d(j)\}$ as:

$$LLSLS.$$

We would like to determine the size and shape of the sets $\mathcal{D}$ and $\mathcal{E}$ in general (as these determine the number of generators and embedding dimension, as above). In order to do this we require to know the shapes of our general $\{d(j)\}$ and $\{w(j)\}$.

Let $S_0 = \{*\} = L_0$ (a single digit or element of a block). Then, for $1 \leq k \leq n$, we define recursively:

$$S_1 = S = \{*\}^{q_1}, \qquad L_1 = L = \{*\}^{q_1+1} \tag{1}$$

$$L_k = L_{k-1}S_{k-1}^{q_k} \qquad S_k = L_{k-1}S_{k-1}^{q_k-1} \text{ for even } k \geq 2; \tag{2}$$

$$L_k = S_{k-1}^{q_k}L_{k-1}, \qquad S_k = S_{k-1}^{q_k-1}L_{k-1} \text{ for odd } k \geq 3. \tag{3}$$

Proposition 4. *If $s/p = [0; q_1, \ldots, q_n]$ with $q_n \geq 2$ then the sequence of residues when $h = s$ gives the word S_n.*

Example 5. *As before, let $\frac{s}{p} = \frac{5}{13} = [0; 2, 1, 1, 2]$ and let $h = s$. Then, using these recursive relations:*

$$\begin{aligned} S_4 &= L_3 S_3^{q_4-1} \\ &= S_2^{q_3} L_2 (S_2^{q_3-1} L_2)^{q_4-1} \\ &= (LS^{q_2-1})^{q_3} LS^{q_2} [(LS_2^{q_2-1})^{q_3-1} LS^{q_2}]^{q_4-1} \\ &= (LS^0)^1 LS^0 [(LS^0)^0 LS^1]^1 \\ &= LLSLS \end{aligned}$$

Hence $S_4 = L(LS)^2$, which agrees with our previous example.

- What about when $h \neq s$? In this case the words we obtain to describe the $\{d(j)\}$ will be the word S_n but amalgamated in some way. We therefore invent a co-ordinate system to describe how the word has been shifted:

For co-ordinates $(x_1, \ldots, x_n)$ consider the following Algorithm:

Algorithm 6. ***For even*** *n:*

Step 1. Start with $S_n = L_{n-1}S_{n-1}^{q_n-1}$.

Step 2. Move x_n copies of S_{n-1} right to left.

Step 3. Then move x_{n-1} copies of S_{n-2} left to right.

Step 4. Then move x_{n-2} copies of S_{n-3} right to left.

$$\vdots$$

Step $n+1$. Conclude by moving x_1 copies of $S_0 = *$ left to right.

For odd *n:*

Step 1. Start with $S_n = S_{n-1}^{q_n-1}L_{n-1}$.

Step 2. Move x_n copies of S_{n-1} left to right.

Step 3. Then move x_{n-1} copies of S_{n-2} right to left.

Step 4. Then move x_{n-2} copies of S_{n-3} left to right.

$$\vdots$$

Step $n+1$. Conclude by moving x_1 copies of $S_0 = *$ left to right.

Let z_j be the number of co-ordinates with $x_i = 0$ for all $i < j$. Using the fact (which we won't prove here) $x_i \leq q_i$ with

$$x_i = q_i \quad \Rightarrow \quad x_{i+1} = 0$$

and in particular, $x_n < q_n$. Then:

$$z_{n+1} = 1, \quad z_n = q_n.$$

$$z_{j-1} = q_{j-1}z_j + z_{j+1}.$$

$$s - h = x_1z_2 + x_2z_3 + \ldots + x_{n-1}z_n + x_nz_{n+1}.$$

Theorem 7. *To obtain the sequence $\{d(j)\}$ for $s - h = z_2x_1 + \ldots + z_{n+1}x_n$, i.e. for co-ordinates $(x_1, \ldots, x_n)$, perform Algorithm 6.*

Example 8. $\frac{4}{13} = [0; 3, 4]$. *The co-ordinate (1,3) corresponds to the $\{d(j)\}$:*

1. $S_2 = L_1S_1^{q_2-1} = L_1S_1^3$
2. *Move x_2 copies of S_1 right to left: $S_1^3L_1$*
3. *Move x_1 copies of $S_0 = *$ left to right: since $S_1 = * * *$, we obtain: $\{d(j)\} = * * S_1^2L_1*$*

And this corresponds to which value of h? Well, $z_3 = 1$, $z_2 = q_2$ thus $f_1 = q_1 f_2 + f_3 = 13$. So

$$s - h = x_1 s + x_2 = 4 + 3 = 7,$$

or $h = -3$.

In a similar manner, we can obtain co-ordinates for each value of h in the example:

$s-h$	$d(j)$	Co-ord
0	$LSSS$	$(0,0)$
1	$SLSS$	$(0,1)$
2	$SSLS$	$(0,2)$
3	$SSSL$	$(0,3)$
4	$***SSS*$	$(1,0)$
5	$**LSS*$	$(1,1)$
6	$**SLS*$	$(1,2)$
7	$**SSL*$	$(1,3)$
8	$**SSS**$	$(2,0)$
9	$*LSS**$	$(2,1)$
10	$*SLS**$	$(2,2)$
11	$*SSL**$	$(2,3)$
12	$*SSS***$	$(3,0)$

So now we can describe our $\{d(j)\}$ pattern for varying h using our co-odinate system and 'words'.

Proposition 9. *Let $d_n(j)$ denote the general pattern of the $\{d(j)\}_{0\le j\le p-1}$ for a given n. For $\frac{s}{p} = [0; q_1, \ldots, q_n]$ and co-ordinates $(x_1, \ldots x_n)$ the pattern of the $\{d(j)\}$ for general n are as follows:*

For even n:

$$\begin{aligned} d_n(j) = &\{*\}^{q_1-x_1} S_1^{x_2-1} S_2^{q_3-x_3-1} L_2 S_3^{x_4-1} S_4^{q_5-x_5-1} L_4 \ldots \\ & S_{n-2}^{q_{n-1}-x_{n-1}-1} L_{n-2} S_{n-1}^{x_n-1} L_{n-1} S_{n-1}^{q_n-x_n-1} \ldots \\ & L_5 S_5^{q_6-x_6-1} S_4^{x_5-1} L_3 S_3^{q_4-x_4-1} S_2^{x_3-1} L_1 S_1^{q_2-x_2-1} \{*\}^{x_1}. \end{aligned} \tag{4}$$

For odd n:

$$\begin{aligned} d_n(j) = &\{*\}^{q_1-x_1} S_1^{x_2-1} S_2^{q_3-x_3-1} L_2 S_3^{x_4-1} S_4^{q_5-x_5-1} L_4 \ldots \\ & S_{n-2}^{x_{n-1}-1} S_{n-1}^{q_n-x_n-1} L_{n-1} S_{n-1}^{x_n-1} L_{n-2} S_{n-2}^{q_{n-1}-x_{n-1}-1} \ldots \\ & L_5 S_5^{q_6-x_6-1} S_4^{x_5-1} L_3 S_3^{q_4-x_4-1} S_2^{x_3-1} L_1 S_1^{q_2-x_2-1} \{*\}^{x_1}. \end{aligned} \tag{5}$$

As the $w(j)$ depend on the $d(j)$ we can now find the general pattern of these too:

Proposition 10. *Let $w_n(j)$ denote the general pattern of the $\{w(j)\}_{0\le j\le p-1}$ for a given n. Then:*

$$w_1(j) = *^{\max(q_1-x_1,x_1)} *^{\min(q_1-x_1,x_1)}, \tag{6}$$

and for even n:

$$w_n(j) = L_{n-1} S_{n-1}^{q_n - 2} w_{n-1}(j). \tag{7}$$

For odd $n > 1$, write

$$\alpha = \max(q_n - x_n - 1, x_n - 1)$$
$$\beta = \min(q_n - x_n - 1, x_n - 1)$$

Then:

$$w_n(j) = S_{n-1}^{\alpha} L_{n-1} S_{n-1}^{\beta} w_{n-1}(j). \tag{8}$$

Note that if, for example, $x_4 = 0$, then we will have a negative exponent on the S_3 in (4) and (5). This needs to be reinterpreted in some way so it makes sense. We have been able to do this when thinking about only the $\{d(j)\}$ but it is not yet clear how to obtain the general pattern of the $\mathcal{D}$ and $\mathcal{E}$ when some of the x_i are zero (although we have solved these entirely for $n = 2, 3$). For now, then, we have only the following Propositions:

Proposition 11. *Let none of the x_i be zero. For even n, the set $\mathcal{D}$ can be described as:*

$$\begin{aligned}\mathcal{D} =\{&0, s_1 - x_1 s_0, 2s_1 - x_1 s_0, \ldots, x_2 s_1 - x_1 s_0,\\ &s_3 - x_3 s_2 + x_2 s_1 - x_1 s_0, 2s_3 - x_3 s_2 + x_2 s_1 - x_1 s_0, \ldots,\\ &x_4 s_3 - x_3 s_2 + x_2 s_1 - x_1 s_0, \ldots,\\ &s_{n-1} - x_{n-1} s_{n-2} + x_{n-2} s_{n-3} - \ldots + x_2 s_1 - x_1 s_0, \ldots,\\ &x_n s_{n-1} - x_{n-1} s_{n-2} + x_{n-2} s_{n-3} - \ldots + x_2 s_1 - x_1 s_0\}\end{aligned}$$

Thus, for even n,

$$|\mathcal{D}| = 1 + \sum_{\substack{i<n \\ i \text{ even}}} x_i \tag{9}$$

For odd n, we have the following:

For $x_n < \frac{1}{2} q_n$, D is the same as the even case, i.e. only the even elements are in $\mathcal{D}$.

For $x_n \geq \frac{1}{2} q_n$, $\mathcal{D}$ is the same as the even case, but with one extra element, μ, at the end, where,

$$\mu = s_n - x_n s_{n-1} + x_{n-1} s_{n-2} - x_{n-2} s_{n-3} + \ldots + x_2 s_1 - x_1 s_0.$$

Hence, for odd n:

$$|\mathcal{D}| = \begin{cases} 1 + \sum_{i \text{ even}} x_i & \text{for } x_n < \frac{1}{2} q_n \\ 2 + \sum_{i \text{ even}} x_i & \text{for } x_n \geq \frac{1}{2} q_n \end{cases} \tag{10}$$

Proposition 12. *Let none of the x_i be zero. For even n, the set $\mathcal{E}$ can be described as:*

$$\begin{aligned}\mathcal{E} =\{&0, 1, s_1 + s_0, 2s_1 + s_0, \ldots, q_2 s_1 + s_0,\\ &s_3 + s_2, 2s_3 + s_2, \ldots q_4 s_3 + s_2, \ldots\\ &s_{n-1} + s_{n-2}, 2s_{n-1} + s_{n-2}, \ldots, (q_n - 1)s_{n-1} + s_{n-2},\\ &p - \min(q_{n-1} - x_{n-1}, x_{n-1}) \cdot s_{n-2},\\ &p - \min(q_{n-3} - x_{n-3}, x_{n-3}) \cdot s_{n-4}, \ldots, p - \min(q_1 - x_1, x_1) \cdot s_0\}.\end{aligned}$$

Hence, for even n:

$$|\mathcal{E}| = 1 + \frac{n}{2} + \sum_{i \text{ even}} q_i \tag{11}$$

For odd n:

$$\begin{aligned}\mathcal{E} =& \{0, 1, s_1 + s_0, 2s_1 + s_0, \ldots, q_2 s_1 + s_0,\\ & s_3 + s_2, 2s_3 + s_2, \ldots q_4 s_3 + s_2, \ldots\\ & s_{n-2} + s_{n-3}, 2s_{n-2} + s_{n-3}, \ldots, q_{n-1} s_{n-2} + s_{n-3},\\ & p - \min(q_n - x_n, x_n) \cdot s_{n-1},\\ & p - \min(q_{n-2} - x_{n-2}, x_{n-2}) \cdot s_{n-3}, \ldots, p - \min(q_1 - x_1, x_1) \cdot s_0\}.\end{aligned}$$

$$|\mathcal{E}| = 2 + \left\lceil \frac{n}{2} \right\rceil + \sum_{i \text{ even}} q_i \tag{12}$$

Notes:

- *Conjecture: If, for i odd, any $x_i = 0$ then the $p - \min(q_i - x_i, x_i) \cdot s_{i-1}$ term does not appear in $\mathcal{E}$.*
- *Conjecture: we agree with dst07 in that when we have co-ordinate $(x_1, 0, \ldots, 0)$, in fact in their case $x_1 = 1$, we replace x_i by the q_i in our formulae for $\mid \mathcal{D} \mid$.*

Finally, we end on a result that we proved in some earlier work. It is the $\mathrm{char}(K) = p$ equivalent of Ferton's Theorem from 1972, where she gave necessary and sufficient conditions for the freeness of $\mathfrak{P}_L^h$ over $A_{L/K}(\mathfrak{P}_L^h)$ in $\mathrm{char}(K) = 0$. We have shown that her conditions transfer over into charcteristic p:

Proposition 13. *Let $0 \leq h \leq p - 1$:*

1. *If $b \equiv 1 \pmod p$ then $\mathfrak{P}_L^h$ is free over $A_{L/K}(\mathfrak{P}_L^h)$ iff $h = 0$, $h = 1$, $h > \frac{p+1}{2}$.*
2. *If $b \not\equiv 1 \pmod p$ then:*
   (a) *$\mathfrak{P}_L^h$ is not free over $A_{L/K}(\mathfrak{P}_L^h)$ $\forall\ s < h \leq p - 1$.*
   (b) *Let $\frac{s}{p} = [0; q_1, \ldots, q_n]$. For $0 \leq h \leq s$, $\mathfrak{P}_L^h$ is free over $A_{L/K}(\mathfrak{P}_L^h)$ iff*
      - *for n even, $h = s$ or $h = s - q_n$*
      - *for n odd, $s - \frac{1}{2}q_n \leq h \leq s$.*