Some computations with pro-p groups with PARI/GP

Marine Rougnant

Atelier PARI/GP 2017 - Lyon

1. Looking for mild pro-p groups
   - Why ?
   - Where ?
   - How ?

2. Computations and examples
   - Auxiliary Frobenius
   - Examples & Stats
   - Propagation

3. What about the other ones ?
   - A diagram...
   - ... and graphs
   - Examples, again !

Why ?

- $\rightsquigarrow$ Cohomological dimension 2,
- $\rightsquigarrow$ Poincaré series of the graduate algebra $\mathrm{gr}(\mathbb{F}_p[[G]])$ known.

Consider :

- p a prime number,
- $K = \mathbb{Q}$ or K an imaginary quadratic field ($K \neq \mathbb{Q}(j)$ if $p = 3$) with trivial p-class group,
- S a finite set of primes of K with norm 1 modulo p.

- $K_S|K$: the maximal pro-p extension of K unramified outside S.

$$G_S = \mathrm{Gal}(K_S|K)$$

Theorem (Labute-Minac-Schmidt criterion)

Let G be a pro-p group with finite p-rank. If the cohomology groups (over $\mathbb{F}_p$) of G satisfy the following conditions :

- *there exist two $\mathbb{F}_p$-vector spaces U and V such that $H^1(G, \mathbb{F}_p) \simeq U \oplus V$,*
- *the cup-product $\cup : H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ restricted to $V \otimes V$ is identically zero,*
- *the cup-product $\cup : H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ restricted to $U \otimes V$ is surjective,*

then the pro-p group G is mild.

Theorem (LMS criterion)

If there exist two vector spaces U, V such that :

- $H^1(G_S(K)) \simeq U \oplus V$,
- $\cup : V \times V \to^0 H^2(G_S(K))$
- $\cup : U \times V \twoheadrightarrow H^2(G_S(K))$

then the pro-p group $G_S(K)$ is mild.

Theorem (LMS criterion)

If there exist two vector spaces U, V such that :

- $H^1(G_S(K)) \simeq U \oplus V$,
- $\cup : V \times V \to^0 H^2(G_S(K))$
- $\cup : U \times V \twoheadrightarrow H^2(G_S(K))$

then the pro-p group $G_S(K)$ is mild.

$$\begin{array}{ccc} H^2(G_S(K)) & \longrightarrow & \bigoplus_{v \in S} H^2(\overline{G_v}) \, . \\ & \searrow^{\text{res}} \quad \nearrow^{\text{inf}} & \\ & \bigoplus_{v \in S} H^2(G_v) & \end{array}$$

Theorem (LMS criterion)

If there exist two vector spaces U, V such that :

- $H^1(G_S(K)) \simeq U \oplus V$,
- $\cup : V \times V \to^0 H^2(G_S(K)) \hookrightarrow \bigoplus_{v \in S} H^2(\overline{G_v})$,
- $\cup : U \times V \twoheadrightarrow H^2(G_S(K)) \hookrightarrow \bigoplus_{v \in S} H^2(\overline{G_v})$,

then the pro-p group $G_S(K)$ is mild.

$$H^2(G_S(K)) \longrightarrow \bigoplus_{v\in S} H^2(\overline{G_v}) .$$

$$H^2(G_S(K)) \xrightarrow{\text{res}} \bigoplus_{v\in S} H^2(G_v) \xrightarrow{\text{inf}} \bigoplus_{v\in S} H^2(\overline{G_v})$$

Corollary (LMS criterion)

If there exist two vector spaces U, V such that :

- $H^1(G_S(K)) \simeq U \oplus V$,
- $\cup : V \times V \xrightarrow{\quad\quad} {}^0 \bigoplus_{v \in S} H^2(\overline{G_v})$,
- $\cup : U \times V \twoheadrightarrow \bigoplus_{v \in S} H^2(\overline{G_v})$,

then the pro-p group $G_S(K)$ is mild.

Corollary (LMS criterion)

If there exist two vector spaces U, V such that :

- $H^1(G_S(K)) \simeq U \oplus V$,
- $\cup : V \times V \xrightarrow{\quad\quad} {}^0 \bigoplus_{v\in S} H^2(\overline{G_v})$,
- $\cup : U \times V \twoheadrightarrow \bigoplus_{v\in S} H^2(\overline{G_v})$,

then the pro-p group $G_S(K)$ is mild.

Under our hypotheses, we have the decomposition :

$$H^1(G_S) \simeq \bigoplus_{v\in S} H^1(G_v^{p,el}),$$

where $G_v^{p,el}$ is the Galois group of the maximal elementary p-extension of K unramified outside v.

Corollary (LMS criterion respecting S)

If there exist $\mathcal{U}, \mathcal{V}$ such that $S = \mathcal{U} \sqcup \mathcal{V}$ and such that

- $H^1(G_S) \simeq U \oplus V$,
- $\cup : V \times V \xrightarrow{\quad} {}^0 \bigoplus_{v \in S} H^2(\overline{G_v})$,
- $\cup : U \times V \twoheadrightarrow \bigoplus_{v \in S} H^2(\overline{G_v})$,

where $U = \bigoplus_{v \in \mathcal{U}} H^1(G_v^{p,el})$ and $V = \bigoplus_{v \in \mathcal{V}} H^1(G_v^{p,el})$, then the pro-p group G_S is mild and we say that ***the field** K **satisfies the LMS criterion respecting** S.*

$\rightsquigarrow$ Finding a "good basis" of $H^1(G_S)$:

$\rightsquigarrow$ Finding a "good basis" of $H^1(G_S)$:

For each $v \in S$, we choose a prime p_v of K such that :

- p_v is inert in the extension $K_v^{p,el}|K$,
- p_v is totally split in the extension $K_w^{p,el}|K$ $w \in S, w \neq v$.

$\rightsquigarrow$ Computing cup-products :

$\rightsquigarrow$ Computing cup-products :

For a well-chosen basis $\{\widetilde{\chi}_v, v \in S\}$ of $H^1(G_S)$ we have :

Proposition

If v, w in S are such that v is inert in $K_w^{p,el}|K$, then the local component in w of the cup-product $\widetilde{\chi}_w \cup \widetilde{\chi}_v$ is given by the integer l_{vw} such that $Frob_v = Frob_{p_w}^{l_{vw}}$ in $G_w^{p,el}$.

$\rightsquigarrow$ Applying the criterion :

$\rightsquigarrow$ Applying the criterion :

We build a matrix Cup =`cupproduct(K,S,p)` giving each local component (in columns) of each one of the cup-products (in rows) of the family $\{\widetilde{\chi}_v, v \in S\}$.

$\rightsquigarrow$ Applying the criterion :

We build a matrix Cup =`cupproduct(K,S,p)` giving each local component (in columns) of each one of the cup-products (in rows) of the family $\{\widetilde{\chi}_v, v \in S\}$.

Proposition

If there exists an integer $t \in \{1, \dots, |S|\}$ and if we can order the primes of S such that the matrix C of the cup-products $(\widetilde{\chi}_{v_i} \cup \widetilde{\chi}_{v_j})_{i \leqslant t}$ satisfies :

- *the t first rows of C are zero ;*
- *C has rank $|S|$;*

then the pro-p group $G_S(K)$ is mild.

Example

Consider $p = 3$, $K = \mathbb{Q}$, $S = \{\ell_1 = 7, \ell_2 = 13, \ell_3 = 79, \ell_4 = 97\}$.

Example

Consider $p = 3$, $K = \mathbb{Q}$, $S = \{\ell_1 = 7, \ell_2 = 13, \ell_3 = 79, \ell_4 = 97\}$.
$\rightsquigarrow$ *auxiliary primes :* $p_1 = 131$, $p_2 = 433$, $p_3 = 239$ *and* $p_4 = 811$.

Example

Consider $p = 3$, $K = \mathbb{Q}$, $S = \{\ell_1 = 7, \ell_2 = 13, \ell_3 = 79, \ell_4 = 97\}$.

$\rightsquigarrow$ *auxiliary primes :* $p_1 = 131$, $p_2 = 433$, $p_3 = 239$ *and* $p_4 = 811$.

$\rightsquigarrow$ *linking numbers :*

$$\begin{aligned} l_{21} = l_{41} = l_{32} = l_{43} = l_{34} = 0, \\ l_{31} = l_{12} = l_{42} = l_{23} = 1, \\ l_{13} = l_{14} = l_{24} = 2. \end{aligned}$$

Example

Consider $p = 3$, $K = \mathbb{Q}$, $S = \{\ell_1 = 7, \ell_2 = 13, \ell_3 = 79, \ell_4 = 97\}$.

$\rightsquigarrow$ *auxiliary primes :* $p_1 = 131$, $p_2 = 433$, $p_3 = 239$ *and* $p_4 = 811$.

$\rightsquigarrow$ *linking numbers :*

$$\begin{aligned} &l_{21} = l_{41} = l_{32} = l_{43} = l_{34} = 0, \\ &l_{31} = l_{12} = l_{42} = l_{23} = 1, \\ &l_{13} = l_{14} = l_{24} = 2. \end{aligned}$$

$\rightsquigarrow$ *cup-products :*

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{pmatrix}.$$

Example

Consider $p = 3$, $K = \mathbb{Q}$, $S = \{\ell_1 = 7, \ell_2 = 13, \ell_3 = 79, \ell_4 = 97\}$.

$\rightsquigarrow$ *auxiliary primes :* $p_1 = 131$, $p_2 = 433$, $p_3 = 239$ *and* $p_4 = 811$.

$\rightsquigarrow$ *linking numbers :*

$$\begin{aligned} l_{21} &= l_{41} = l_{32} = l_{43} = l_{34} = 0, \\ l_{31} &= l_{12} = l_{42} = l_{23} = 1, \\ l_{13} &= l_{14} = l_{24} = 2. \end{aligned}$$

$\rightsquigarrow$ *cup-products :*

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{pmatrix}.$$

$\rightsquigarrow$ $G_S(K)$ *is mild.*

Example

$S = \{31, 61, 151, 211\}$, $L = \mathbb{Q}(\sqrt{-15})$.
The pro-p group $\mathrm{Gal}(L_S(p)|L)$ *is mild for* $p = 3$ *and* $p = 5$.

Example

$S = \{31, 61, 151, 211\}$, $L = \mathbb{Q}(\sqrt{-15})$.
The pro-p group $\mathrm{Gal}(L_S(p)|L)$ *is mild for* $p = 3$ *and* $p = 5$.

Example

$p = 3$, $S = \{7, 13, 79, 97\}$.
The pro-p group $\mathrm{Gal}(L_S|L)$ *is mild if* $L = \mathbb{Q}(\sqrt{-d})$ *with*
$d \in \{66, 94, 185, 285, 290, 355, 391, 454, 458, 521, 607, 614, 647, 703, 829, 881, 906\}$.

Example

$S = \{31, 61, 151, 211\}$, $L = \mathbb{Q}(\sqrt{-15})$.
The pro-p group $\mathrm{Gal}(L_S(p)|L)$ *is mild for* $p = 3$ *and* $p = 5$.

Example

$p = 3$, $S = \{7, 13, 79, 97\}$.
The pro-p group $\mathrm{Gal}(L_S|L)$ *is mild if* $L = \mathbb{Q}(\sqrt{-d})$ *with*
$d \in \{66, 94, 185, 285, 290, 355, 391, 454, 458, 521, 607, 614, 647, 703, 829, 881, 906\}$.

Example

$S = \{37, 103, 127, 139\}$, $L = \mathbb{Q}(\sqrt{-d})$ *a quadratic field with trivial p-class group in which every prime of S splits.*
If $p = 3$ *and* $d < 10^3$*, then the pro-p group* $\mathrm{Gal}(L_S|L)$ *is mild.*

Suppose that $\mathbb{Q}$ satisfies LMS respecting S. How does this property propagate in quadratic imaginary fields with trivial p-class group, if every element of S splits ?

Suppose that $\mathbb{Q}$ satisfies LMS respecting S. How does this property propagate in quadratic imaginary fields with trivial p-class group, if every element of S splits ?

Let $\mathbb{E}_S$ be the set of the discriminants of all these quadratic fields. We compute the proportion :

$$P_{S,p}(X) = \frac{\#\{d \leqslant X \mid d \in \mathbb{E}_S, \text{prop. 2.2 applies to } \mathbb{Q}(\sqrt{-d})\}}{\#\{d \leqslant X \mid d \in \mathbb{E}_S\}}.$$

S	$P_{S,3}(10^5)$
$\{13, 127, 193, 349\}$	$\simeq 0.8735$
$\{67, 157, 337, 421\}$	$\simeq 0.8619$
$\{31, 79, 199, 409\}$	$\simeq 0.8455$
$\{337, 349, 379, 463\}$	$\simeq 0.8560$
$\{37, 103, 127, 139\}$	$\simeq 0.8879$
$\{97, 151, 313, 457\}$	$\simeq 0.8645$

S	$P_{S,5}(10^4)$
$\{101, 131, 211, 251\}$	$\simeq 0.6667$
$\{11, 31, 41, 211\}$	$= 0.696$
$\{31, 181, 191, 271\}$	$\simeq 0.6744$
$\{211, 251, 401, 421\}$	$\simeq 0.6578$

S	$P_{S,3}(10^6)$
$\{7, 13, 79, 97\}$	$\simeq 0.8655$
$\{43, 61, 157, 337\}$	$\simeq 0.8920$

We now consider :

- L quadratic imaginary field with trivial p-class group ($L \neq \mathbb{Q}(j)$ if $p = 3$),
- S finite set of primes, all equal to 1 modulo p and split in $L|\mathbb{Q}$.

Denote $G_S = G_S(\mathbb{Q})$ and $H_S = G_S(L)$.

We now consider :

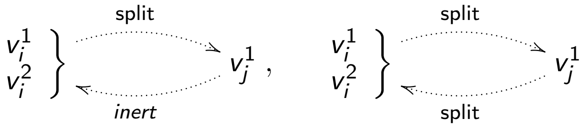
- L quadratic imaginary field with trivial p-class group ($L \neq \mathbb{Q}(j)$ if $p = 3$),
- S finite set of primes, all equal to 1 modulo p and split in $L|\mathbb{Q}$.

Denote $G_S = G_S(\mathbb{Q})$ and $H_S = G_S(L)$.

$$\begin{array}{ccccc}
H^1(H_S) \times H^1(H_S) & \xrightarrow{\;\cup\;} & H^2(H_S) & \xrightarrow{\;\inf\cdot\mathrm{res}\;} & \bigoplus_{w \in S'} H^2(\overline{H_w}) \\
\uparrow{\scriptstyle \inf} & & \uparrow{\scriptstyle \inf} & & \uparrow{\scriptstyle \inf} \\
H^1(G_S) \times H^1(G_S) & \xrightarrow{\;\cup\;} & H^2(G_S) & \xrightarrow{\;\inf\cdot\mathrm{res}\;} & \bigoplus_{v \in S} H^2(\overline{G_v}).
\end{array}$$

Suppose that $\mathbb{Q}$ satisfies LMS respecting S for the decomposition $H^1(G_S) = U \oplus V$.
We define two directed graphs $\mathcal{G}_S$ and $\mathcal{G}_S^*$ with vertices the primes of S as follow :

- $\mathcal{G}_S$ has a directed edge (v_i, v_j) from v_i to v_j if :



if $v_i \in \mathcal{V}$ and $v_j \in \mathcal{U}$ if $v_i \in \mathcal{U}$ and $v_j \in \mathcal{V}$

- $\mathcal{G}_S^*$ has a directed edge (v_i, v_j) from v_i to v_j if (v_j, v_i) is an edge of $\mathcal{G}_S$.

A graph is said to be **quasi-circular** if it admits a spanning subgraph in which every vertex is of incoming degree 1.

A graph is said to be **quasi-circular** if it admits a spanning subgraph in which every vertex is of incoming degree 1.

Theorem

If $\mathbb{Q}$ satisfies LMS respecting S and if one of the graphs $\mathcal{G}_S$ or $\mathcal{G}_S^*$ is quasi-circular, then the group H_S satisfies LMS.

A graph is said to be **quasi-circular** if it admits a spanning subgraph in which every vertex is of incoming degree 1.

Theorem

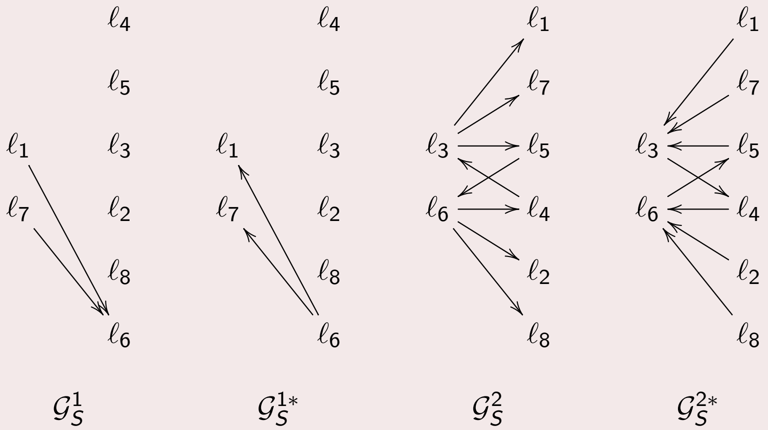
If $\mathbb{Q}$ satisfies LMS respecting S and if one of the graphs $\mathcal{G}_S$ or $\mathcal{G}_S^*$ is quasi-circular, then the group H_S satisfies LMS.

Corollary

When $|S| = 4$, the group H_S satisfies LMS if the graph $\mathcal{G}_S$ admits an elementary circuit (of length 4) as a spanning subgraph.

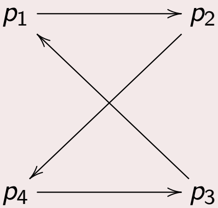
Example

$S = \{7, 43, 61, 103, 109, 163, 223, 241\}$, $L = \mathbb{Q}(\sqrt{-5})$, $p = 3$.

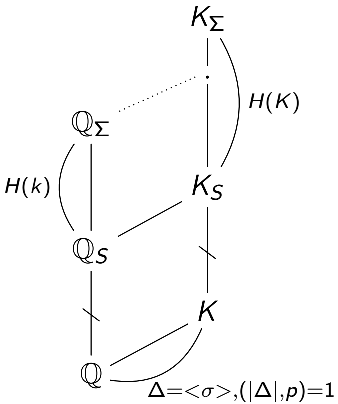


Example

$p = 3, S = \{61, 223, 229, 487\}, d = 5,$
We obtain the following graph $\mathcal{G}_S$:



The pro-p group H_S is mild, even if the field L does not satisfy LMS respecting S ("crossed" cup-products have rank 7).



where :

- K a cyclic extension of degree ℓ of $\mathbb{Q}$,
- S a finite set of primes such that $G_S(\mathbb{Q}) \simeq G_S(K)$,
- Σ a finite set of primes containing S and p,
- ℓ an integer coprime to p.

Thanks for your attention !