

Geometric interpretation of quadratic Chabauty. Bas Edixhoven.

Seminaire Variétés Rationnelles, 2018/10/19, Paris IHP, 50th birthday P. Gille.

(Joint work with Guido Lido.) Still quite preliminary, no example worked out yet, nothing really written yet (well: notes of Oberwolfach lecture)

Goal: to replace p-adic Hodge theory, p-adic heights, p-adic ^{integration} and ~~not geom.~~ by "old-fashioned" (1980's) algebraic geometry / \mathbb{Z} and over $\mathbb{Z}/p^2\mathbb{Z}$, not to reprove finiteness statements but to find $C(\mathbb{Q})$ for specific C .

Note: we are re-interpreting the work of Balakrishnan, Dogra, Müller, Tuitman and Vonk. Hopefully, computations become easier, and we clarify what quadr. Chabauty "is".

Let C/\mathbb{Z} be a curve, proper, flat, regular, $C_{\mathbb{Q}}$ geom. connected, genus $g \geq 2$, $n \geq 1$ s.t. C smooth over $\mathbb{Z}[1/n]$.

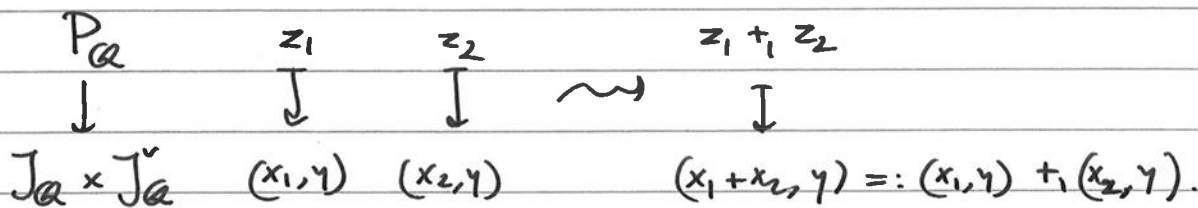
$J :=$ Néron model / \mathbb{Z} of $\text{Pic}_{C_{\mathbb{Q}}/\mathbb{Q}}^0$, $J^{\vee} :=$ Néron model / \mathbb{Z} of $J_{\mathbb{Q}}^{\vee}$, \checkmark . $1: J \rightarrow J^{\vee}$

$B_{\mathbb{Q}} :=$ Poincaré line bundle on $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$, trivialised on $(\{0\} \times J_{\mathbb{Q}}^{\vee}) \cup (J_{\mathbb{Q}} \times \{0\})$.

$P_{\mathbb{Q}} :=$ Poincaré \mathbb{G}_m -torsor on $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$: $P_{\mathbb{Q}} = \underline{\text{Isom}}_{J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}}(0, B_{\mathbb{Q}})$.

$P_{\mathbb{Q}}$ is a bi-extension of $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$ by \mathbb{G}_m : for S a \mathbb{Q} -scheme, $x_1, x_2 \in J_{\mathbb{Q}}(S)$, $y \in J_{\mathbb{Q}}^{\vee}(S)$: $(x_1 + x_2, y)^* B_{\mathbb{Q}} = (x_1, y)^* B_{\mathbb{Q}} \otimes_S (x_2, y)^* B_{\mathbb{Q}}$, canonical isom from the thm. of the square/cube.

This gives $(x_1 + x_2, y)^* P_{\mathbb{Q}} \leftarrow (x_1, y)^* P_{\mathbb{Q}} \times_S (x_2, y)^* P_{\mathbb{Q}}$



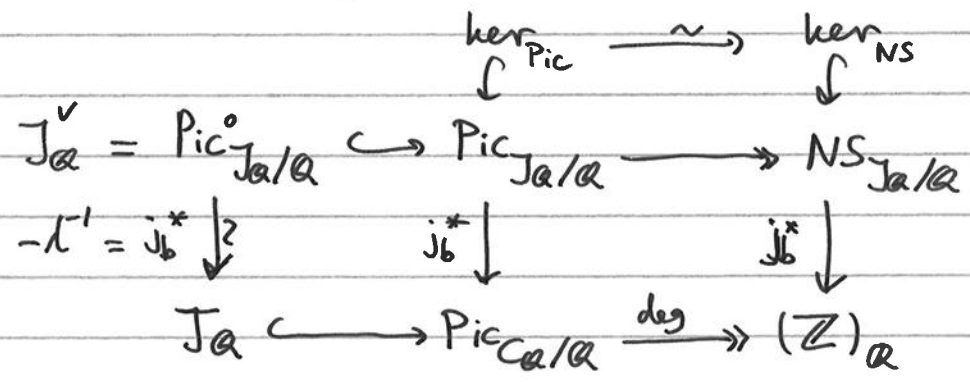
And of course the same for the other coordinate.

These $+_1$ and $+_2$ commute when it makes sense.

Extension over \mathbb{Z} . $J^\circ \hookrightarrow J \twoheadrightarrow \Phi$, with J° irreducible connected component of o of J , Φ finite skyscraper group scheme supported on $\text{Spec}(\mathbb{Z}/n\mathbb{Z})$. Then P_α extends uniquely to $P \rightarrow J \times J^{\vee 0}$ as biextension by \mathbb{G}_m . (obstruction is Grothendieck's pairing $\Phi \times \Phi^\vee \rightarrow \mathcal{O}_e$)
 (Ref: L. Moret-Bailly's "Mémories permises".)
 ("Pinces aux de var. ab.")

Assume: we have $b \in C_\alpha(\mathbb{Q}) (= C(\mathbb{Z}) = C^{sm}(\mathbb{Z}))$. (SGA7)

Then $j_b: C^{sm} \rightarrow J$, $P \mapsto [P-b]$. That gives:

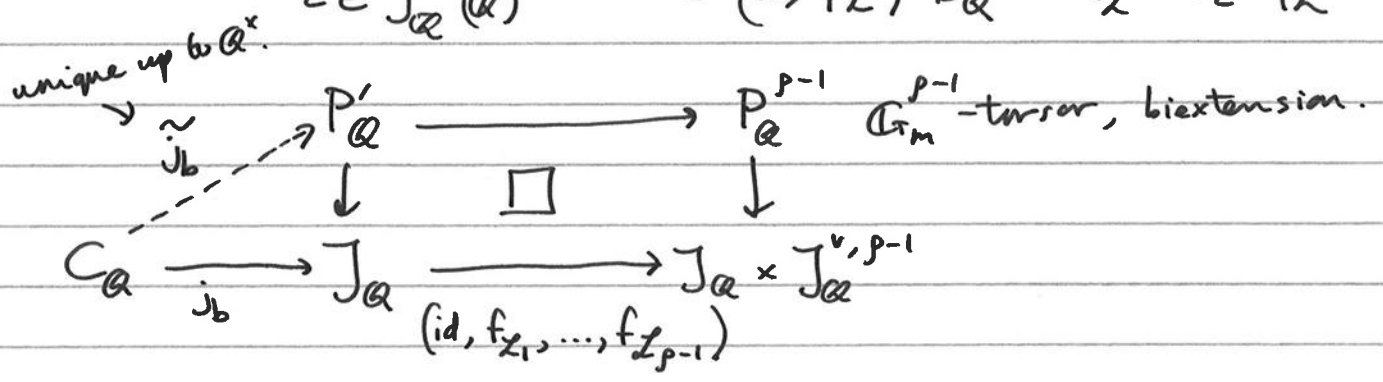


Note: $NS_{J_\alpha/\mathbb{Q}}(\mathbb{Q}) = \text{End}(J_\alpha)^+ \rightarrow \mathbb{Z}$ via trace on $H_1(J(\mathbb{C}), \mathbb{Z})$.
 \uparrow free \mathbb{Z} -module, $\rho := \text{rank}$.

So: $\ker(j_b^*: Pic(J_\alpha) \rightarrow Pic(C_\alpha))$ is free \mathbb{Z} -mod. rank $\rho-1$;
 let $L_1, \dots, L_{\rho-1}$ be a basis, each L_i rigidified at o .

Now we relate this to P_α . For all \mathcal{L} inv. \mathcal{O} -module on J_α we have $\varphi_{\mathcal{L}}: J_\alpha \rightarrow J_\alpha^\vee$, $x \mapsto (\text{tr}_x^* \mathcal{L}) \otimes \mathcal{L}^{-1}$, and

$$\mathcal{L}^{\otimes 2} = \underbrace{\mathcal{L} \otimes (\text{id})^* \mathcal{L}^{-1}}_{\in J_\alpha^\vee(\mathbb{Q})} \otimes \underbrace{\mathcal{L} \otimes (-\text{id})^* \mathcal{L}}_{\in (\text{id}, \varphi_{\mathcal{L}})^* B_\alpha} = (\text{id}, f_{\mathcal{L}})^* B_\alpha \text{ with } f_{\mathcal{L}} = \text{tr}_C \circ \varphi_{\mathcal{L}}.$$

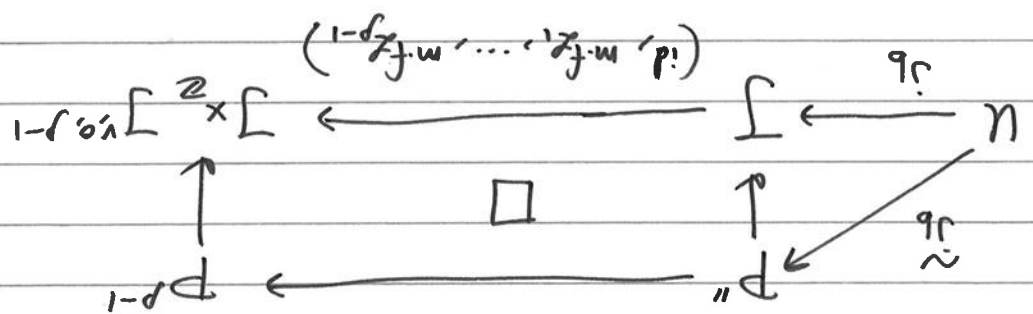


3. V_i, f_i extends uniquely to $f_i: J \rightarrow J'$.

Let $m := \text{l.c.m. of the exponents of the } \Phi(\mathbb{F}_p), p \mid n$.
 Then $m \cdot f_i: J \rightarrow J'$, and $(\text{id}, m \cdot f_i)^* B_{\mathbb{Q}} = X_i^{2m}$: trivial on \mathbb{C}^* .

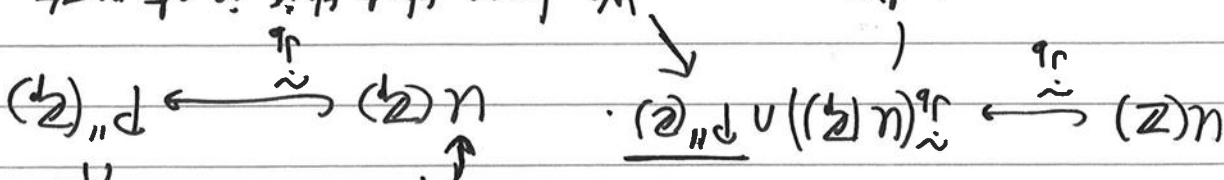
$j'_i: C^{sm} \rightarrow J$, $j'_i^* (\text{id}, m_i \cdot f_i)^* B$ is trivial, uniquely up to ± 1 .

on each of the finitely many open $U \subset C^{sm}$ obtained by removing all but one irred. comp. of each of the reducible fibres of $C^{sm} \rightarrow \text{Spec}(\mathbb{Z})$.
 Note: every $P \in C(\mathbb{Q})$ extends uniquely to a $P \in U(\mathbb{Z})$ for a unique U .
 For each such U we have:



Note that $P''(\mathbb{Z}) \rightarrow J(\mathbb{Z})$ is a (± 1) -torsor.

Now we apply Chabauty's idea:

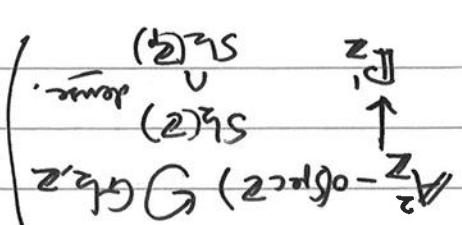


We hope that this is at most r -dimensional. $\dim P''(\mathbb{Z}) = g + p - 1$.
 $r = \text{rank}(J(\mathbb{Z}))$.

Chabauty's idea should work if $r < g + p - 1$.

The hierarchy structure of P^{p-1} should help us to understand $P''(\mathbb{Z}) \subset P''(\mathbb{Q})$.

(Note: oh, a rational variety!)
 Without such a structure it doesn't work.



How can we parametrise $P''(\mathbb{Z})$?

Let $P_1, \dots, P_r, \dots, P_s$ generate $J(\mathbb{Z})$, Q_1, \dots, Q_t generate $J^{v,0}(\mathbb{Z})$.

Recall: $m \cdot f_{\mathbb{Z}_k} = m \cdot (\text{tr}_{\mathbb{Z}_k} \circ \varphi_{\mathbb{Z}_k}) = \text{tr}_{m \cdot \mathbb{Z}_k} \circ m \cdot \varphi_{\mathbb{Z}_k}$.

$\forall i, \forall k$, write $m \cdot \varphi_{\mathbb{Z}_k}(P_i) = \sum_j a_{k,i,j} \cdot Q_j$,

$\forall k$, write $m \cdot c_k = \sum_j b_{k,j} Q_j$.

$\forall i, j$ let $R_{i,j} \in P(\mathbb{Z})$ over (P_i, Q_j) in $(J \times J^{v,0})(\mathbb{Z})$.

Then, $\forall n_1, \dots, n_s \in \mathbb{Z}$, $\sum_i n_i P_i$ in $J(\mathbb{Z})$ is mapped to

$\left(\sum_i n_i P_i, \left(\sum_j (b_{k,j} + \sum_i n_i a_{k,i,j}) Q_j \right)_{k=1}^{p-1} \right)$ in $(J \times J^{v,0,p-1})(\mathbb{Z})$.

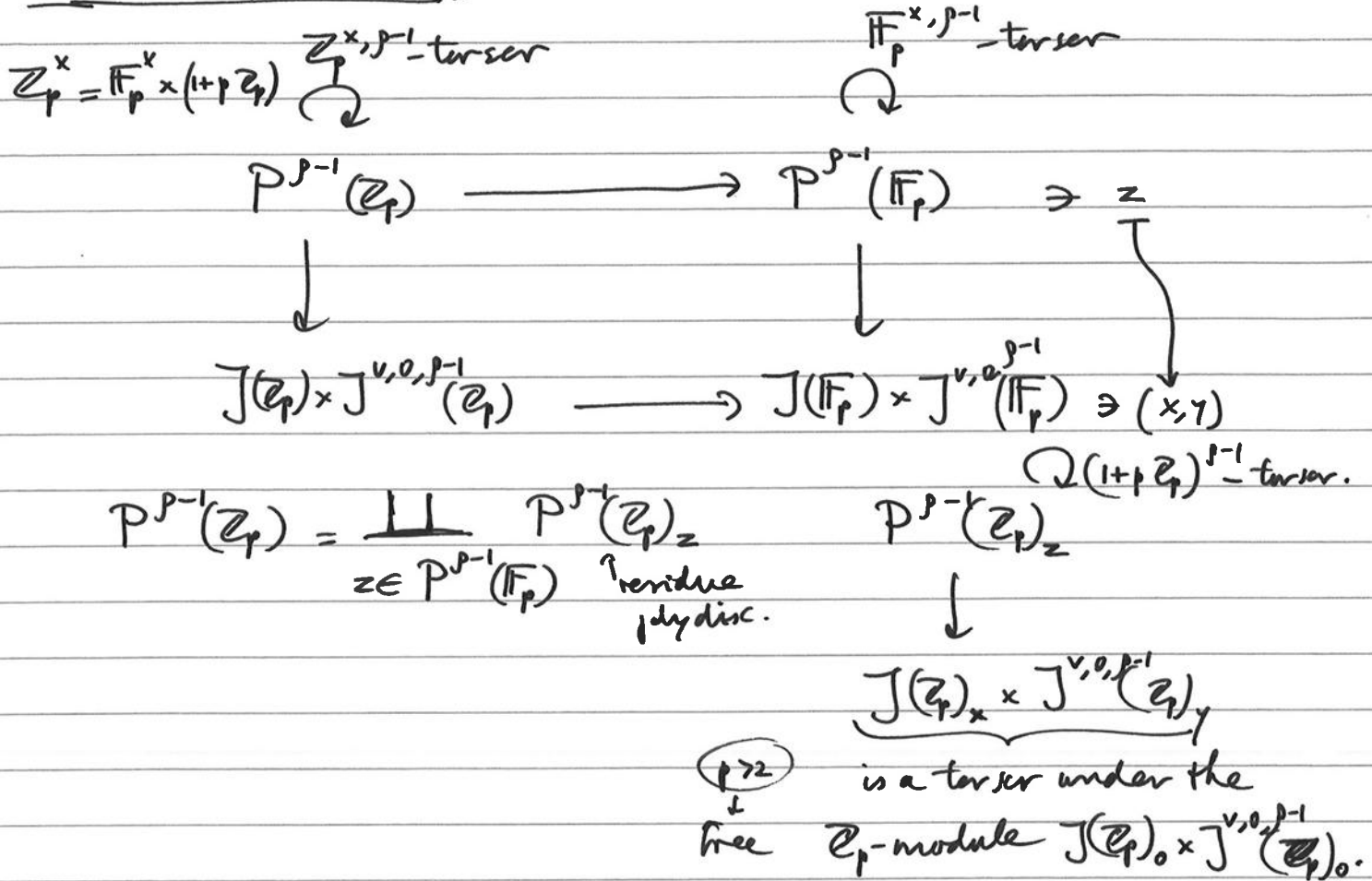
Over this, in $P^{p-1}(\mathbb{Z})$, we have:

$\left(\sum_j \left(b_{k,j} + \sum_i n_i a_{k,i,j} \right) \cdot \underbrace{\left(\sum_i n_i R_{i,j} \right)}_{\text{over } (\sum n_i P_i, Q_j)} \right)_{k=1}^{p-1}$

Note that this is quadratic in the n_i .

Idea to see the closure in $P''(\mathbb{Z}_p)$: think of the $n_i \in \mathbb{Z}_p$.

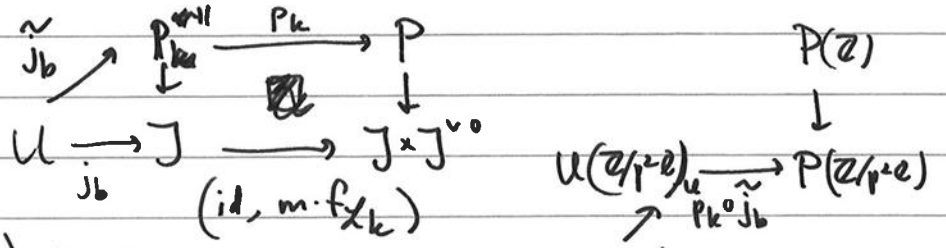
Structure of $P^{p-1}(\mathbb{Z}_p)$



A specific case Assume $r=g, p-1 \geq 2, p > 2, p \nmid n$,
 P_1, \dots, P_g a \mathbb{Z} -basis of $\ker(J(\mathbb{Z}) \rightarrow J(\mathbb{F}_p))$,
 Q_1, \dots, Q_g a \mathbb{Z} -basis of $\ker(J^{v,0}(\mathbb{Z}) \rightarrow J^{v,0}(\mathbb{F}_p))$,
 the images of P_1, \dots, P_g in $\ker(J(\mathbb{Z}/p^2\mathbb{Z}) \rightarrow J(\mathbb{F}_p))$ form an \mathbb{F}_p -basis,
 and same for the Q_1, \dots, Q_g .

Then, $\forall u \in U(\mathbb{F}_p)$ s.t. $\tilde{j}_b(u) \in P''(\mathbb{F}_p)$ is in the image of $P''(\mathbb{Z})$,

$\forall k \in \{1, \dots, p-1\}$,



$(P_k \circ \tilde{j}_b)^{-1}$ (image of $P(\mathbb{Z})$) is given by a quadr. equation, on $T_{U(\mathbb{F}_p)}(u)$, to which Hensel is applicable at most unique p -adic lifts of simple zeros over \mathbb{F}_p .