Chabauty's method and beyond, by Bas Edixhoven, universiteit Leiden, NL.

Finding <u>all</u> rational solutions of a polynomial equation $(x,y)=0$ with rational coefficients can be a difficult problem.

An example of this is the case of the so-called "cursed curve", given by the equation:

$$-(y+1)\cdot x^3 + (2y^2+y)\cdot x^2 + (-y^3+y^2-2y+1)\cdot x + (2y^2-3y)\cdot 1 = 0.$$

On this curve, number 1 on the "most wanted list" for a reason that one could also talk about, there were 7 known rational points: $(0,0)$, $(1,0)$, $(-1,0)$, $(0,3/2)$ and the points "at infinity" in the projective plane $(1:0:0)$, $(1:1:0)$ and $(0:1:0)$. For a long time the curve resisted all attackers who wanted to prove that there are no other rational points, whatever tools they brought. The solution came in 2017, published in the Annals of Mathematics in 2019. A team of 5 mathematicians, Balakrishnan, Dogra, Müller, Tuitman and Vonk, had built a new weapon, called "quadratic Chabauty", by implementing the simplest non-linear case of Minhyong Kim's "nonabelian Chabauty" method. In the last 2 years, with Guido Lido, we have made this method much much simpler, the result is now in our preprint on arxiv. In the talk I will address the history of this ancient subject, and try to explain the special role of p-adic numbers (that I will also explain) in Chabauty's method, and what happens in the quadratic case.

Colloquium Mainz.

January 30, 2020.

Geometric Quadratic Chabauty, 1.

(jt. work with Guido Lido).

C nice curve / $\mathbb{Q}$, assume $b \in C(\mathbb{Q})$.

$g > 1$.

$j_b : C \longrightarrow J$, $P \mapsto \mathcal{O}_C(P - b)$.

Chabauty has problem if $r \neq g$.

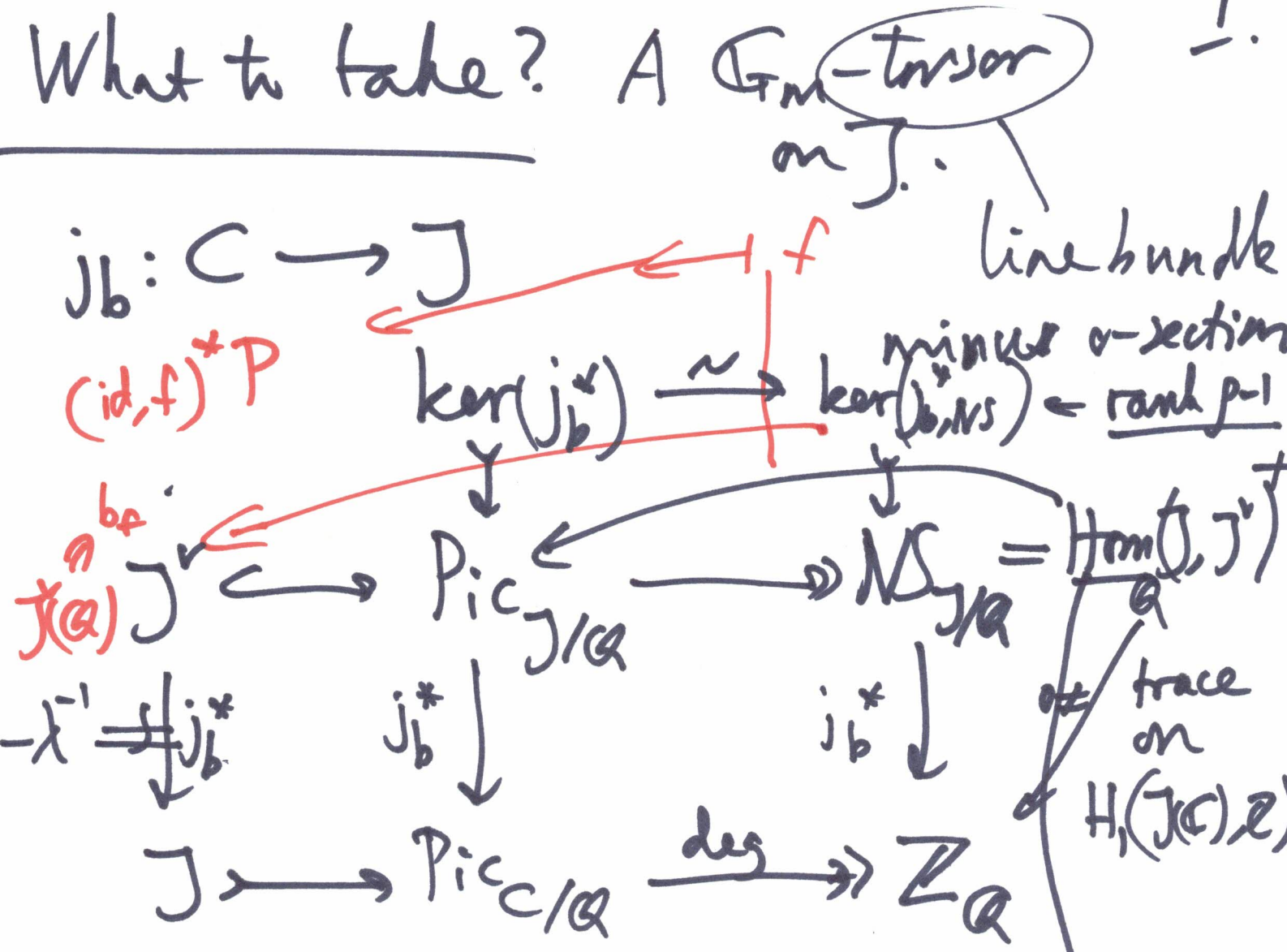
$$\begin{array}{ccc} C(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}) \\ \downarrow & & \cap \\ & & \overline{J(\mathbb{Q})} \\ C(\mathbb{Q}_p) & \longrightarrow & J(\mathbb{Q}_p) \end{array}$$

$\overline{J(\mathbb{Q})}$ can be equal.

Idea: replace J by something bigger, higher dimension, and then play Chab game.

What to take?

A $\mathbb{G}_m$-torsor on J.



Given $f : J \to J^\vee$ with trace 0,
get a line bundle on J
that is trivial on $j_b(C)$.

Poincaré bundle.

$\forall$ ab. var. A, can view $A^\vee$ as $\mathrm{Ext}^1(A, \mathbb{G}_m)$. $\mathbb{G}_m \hookrightarrow E \twoheadrightarrow A$

So over $A^\vee$ have univ. extension:

are rigid. no non-trivial autom. that induce id_A and $\mathrm{id}_{\mathbb{G}_m}$.

$\mathbb{G}_m$, A torsor.

$$\begin{array}{ccc} \mathbb{G}_m & \hookrightarrow & P^\times \\ & \searrow & \downarrow \\ & & A^\vee \end{array} \qquad P^\times \twoheadrightarrow A \times A^\vee \swarrow$$

$P^\times$ is also the univ. ext. of $A^\vee$ by $\mathbb{G}_m$, over A.

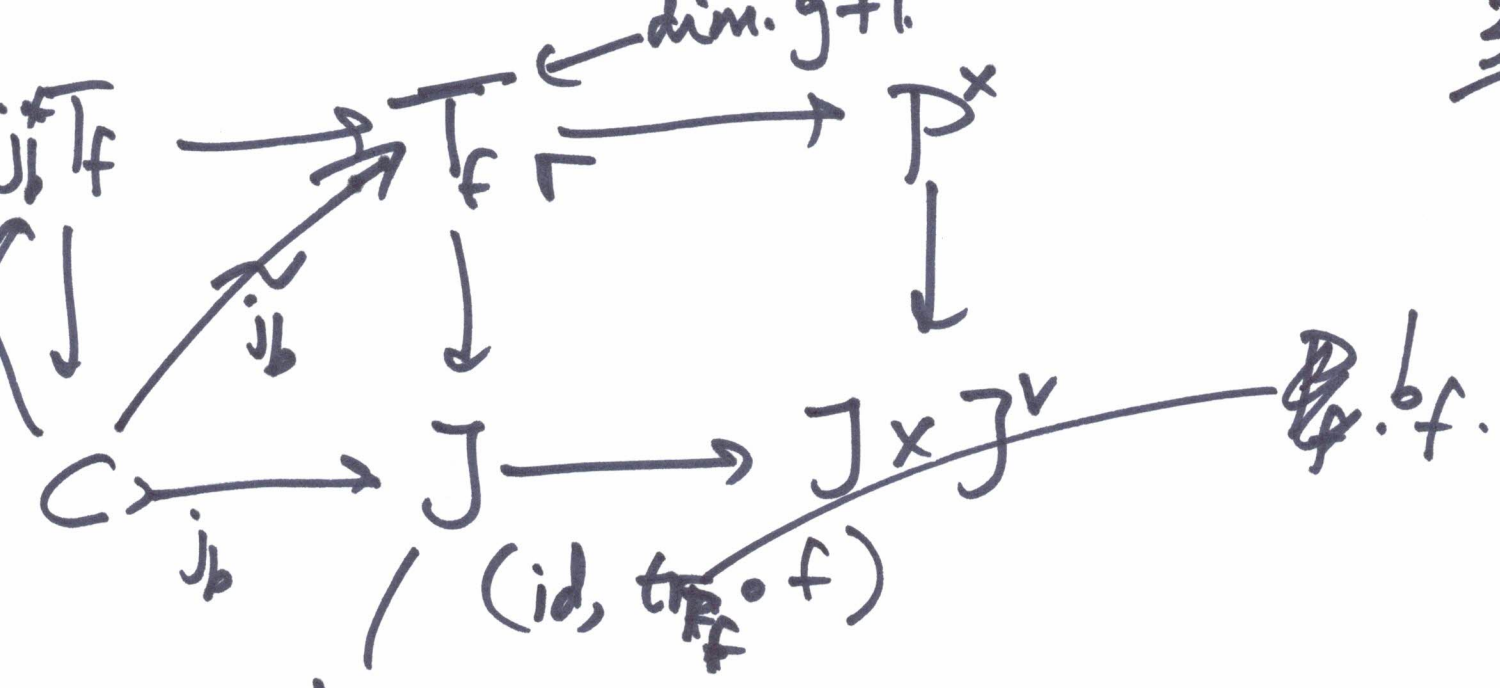
$P^\times$ is a $\mathbb{G}_m$-biextension of $A \times A^\vee$:

2 partial gr. laws: $z_1 +_1 z_2 \in P^\times(x_1+x_2, y)$

$x_1, x_2 \in A$, $y \in A^\vee$

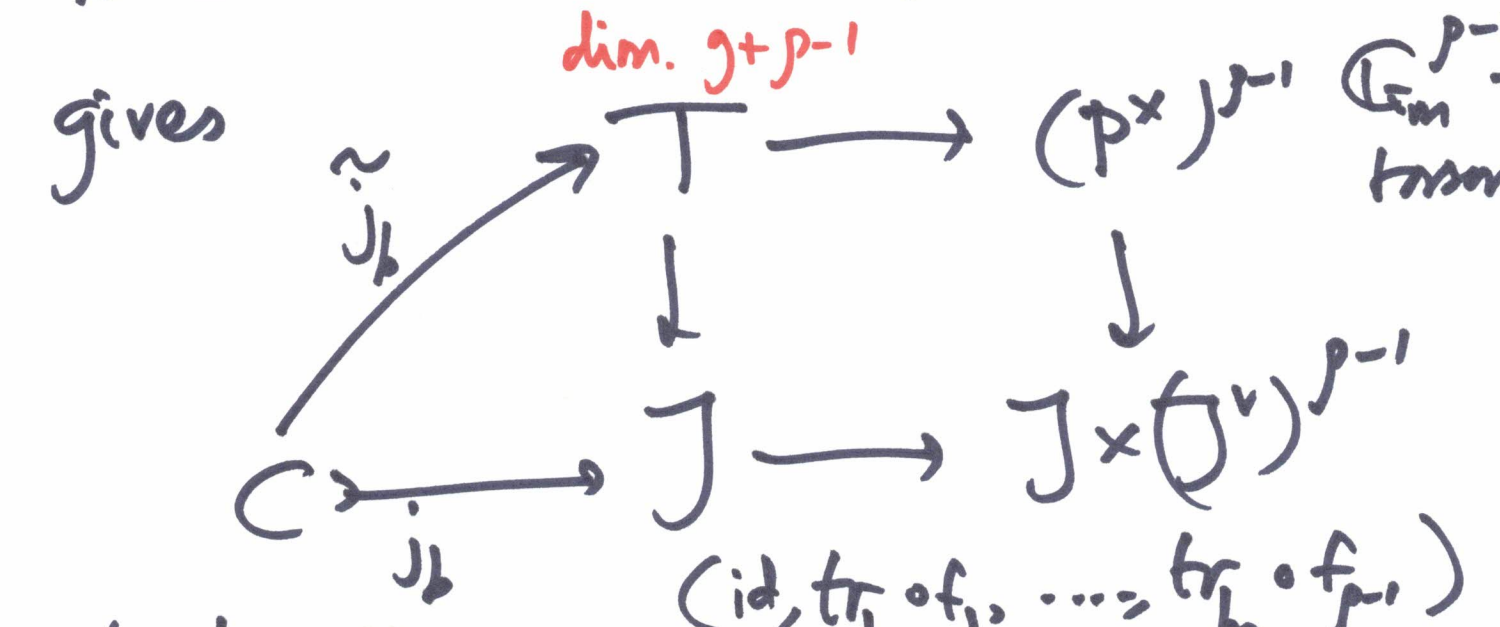
$(x_1, y) \in A \times A'$ $z_1 \in P^\times(x_1, y)$

$(x_2, y) \in$ $z_2 \in P^\times(x_2, y)$



Take a $\mathbb{Z}$-basis $f_1, \dots, f_{p-1}$ of $\ker(j_b^* NS)$,

gives



We play the Chabauty game in T.

Hope that it works if $r < g+p-1$.

(most wanted ex. have $p = g$.)

$T(\mathbb{Q})$ is a $\mathbb{Q}^\times, \rho^{-1}$-torsor.

$\downarrow$

$J(\mathbb{Q})$

$$\mathbb{Q}^\times = \{\pm 1\} \times \mathbb{Z}^{(\text{set of primes})}$$

Big problem, too many $\mathbb{Q}$-points in T.

Solution: extend the geometry over $\mathbb{Z}$. $\mathbb{Z}^\times = \{\pm 1\}$.

From now on everything over $\mathbb{Z}$.

$\mathcal{C}$ proper regular model of $C_{\mathbb{Q}}$.

$\mathcal{J} :=$ Néron model of $J_{\mathbb{Q}}$.

$\mathcal{J}^v :=$ ——— $J^v_{\mathbb{Q}}$, $\mathcal{J}^{v,0} \subset \mathcal{J}^v$:

fibrewise conn. comp. of e.

$P^\times$: unique extension of $P^\times_{\mathbb{Q}}$ to $\mathcal{J} \times \mathcal{J}^{v,0}$ as bi-extension.

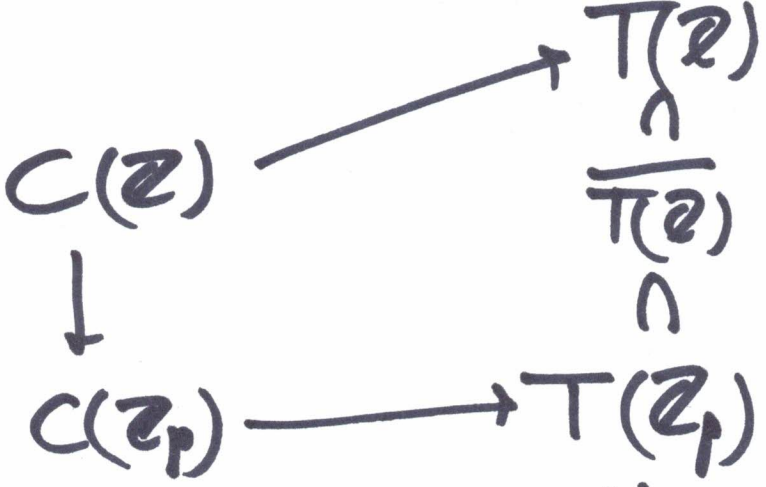
We use the biext. str. of $P^\times$ over $J \times J^{\nu,0}$ to parametrize.

$T(\mathbb{Z})_{(\pm 1)}^{p-1}$ — tensor.

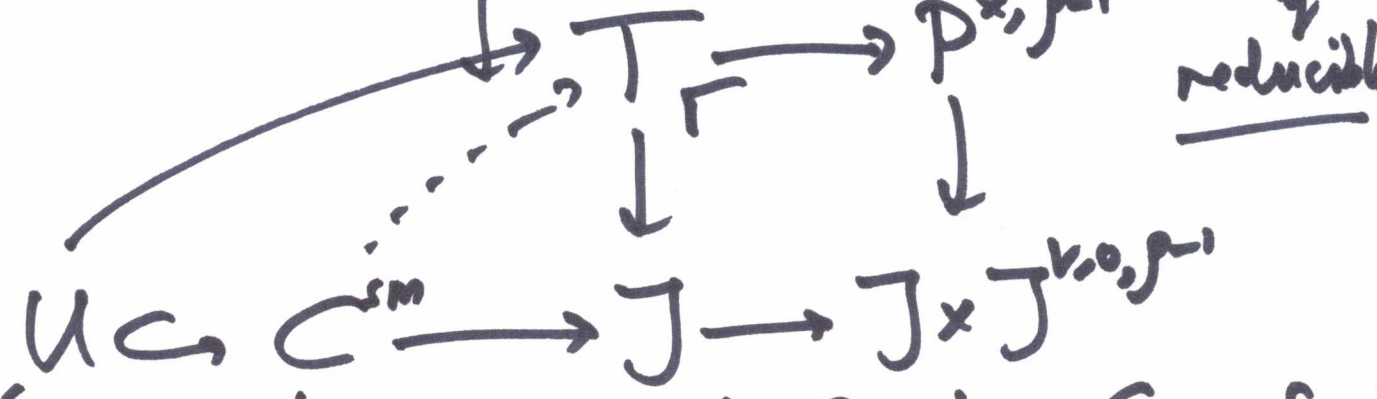
$\vdots$

$J(\mathbb{Z})$

$$\begin{array}{ccc} C(\mathbb{Z}) & \longrightarrow & T(\mathbb{Z}) \\ & & \cap \\ & & \overline{T(\mathbb{Z})} \leq r\text{-dim.} \\ \downarrow & & \cap \\ C(\mathbb{Z}_p) & \longrightarrow & T(\mathbb{Z}_p) \\ \text{1-dim.} & & g+p-1\text{-dim.} \end{array}$$



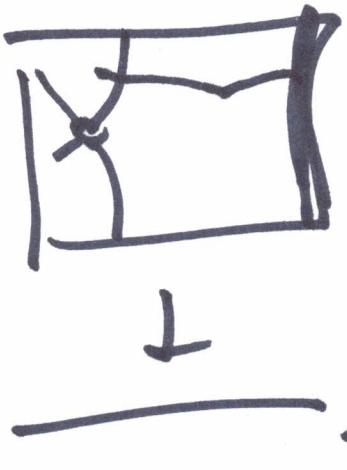
came from problem with primes q s.t $C^{sm}_{\mathbb{F}_q}$ reducible



open subsch. of C where $C \to \operatorname{Spec}\mathbb{Z}$ is smooth

open subsets of C^{sm} obtained by removing in all fibres over closed pts of $\operatorname{Spec}\mathbb{Z}$ all irred. comp. except 1 that is geom. irred.

For $P \in C(\mathbb{Z}) = C^{sm}(\mathbb{Z})$, P selects 1 geom. irr. comp. in each fibre



Say n = prod. of primes q of bad red. of $C/\mathbb{Q}$. Then $C \to \operatorname{Spec}\mathbb{Z}$ is smooth over $\mathbb{Z}[1/n]$.

There are finitely many of such U's, and $C_{\mathbb{Q}}(\mathbb{Q}) = C^{sm}(\mathbb{Z}) = \coprod_{\text{all } U\text{'s}} U(\mathbb{Z})$.

Ex in §8. $y^2+y = x^6+\cdots$

$n = 3.43$ $C^{sm}_{\mathbb{F}_{43}}$ irred. $C^{sm}_{\mathbb{F}_3}$:

$\exists$ exactly 2 U's.

$J^{v,0} \hookrightarrow J^v \twoheadrightarrow \Phi^v$ ← gr. sch. of components of J^v

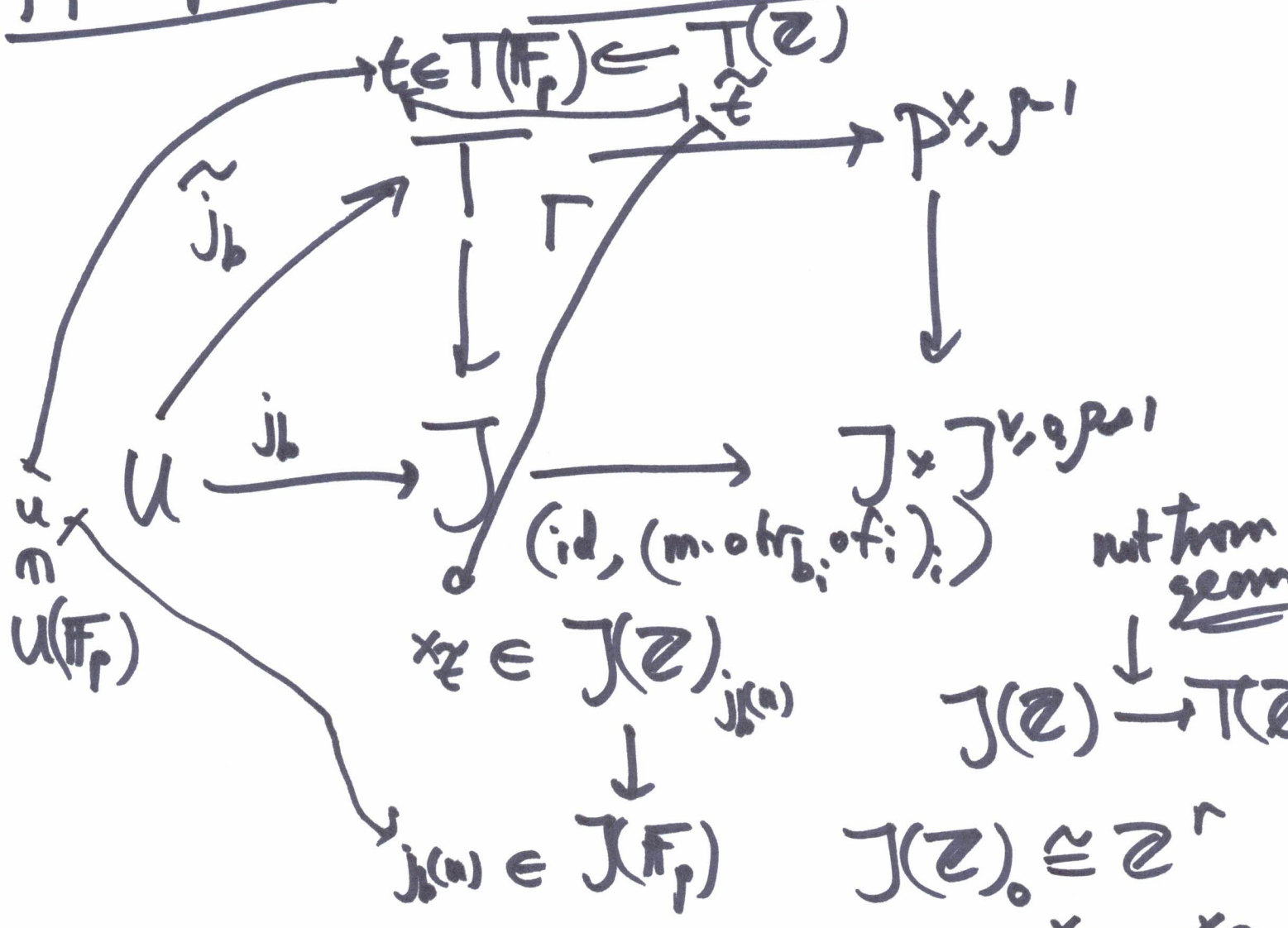
Φ^v trivial over $\mathbb{Z}[1/n]$

finite etale fibres over $\mathbb{Z}/n\mathbb{Z}$

$m :=$ l.c.m. of the ~~orders~~ exponents of $\Phi^v(\overline{\mathbb{F}_q})$, q/n

$$T(\mathcal{Z}) \hookrightarrow \overline{T(\mathcal{Z})} \subset T(\mathbb{Z}_p)$$

$p \nmid n$, $p > 2$. ↑ how to describe this?



We get a map

$$\kappa_{\mathcal{Z}} : \mathcal{Z}^r \longrightarrow T(\mathcal{Z})_t$$

not really surjective.

Thm 4.10.

evaluate $\frac{1}{p}$ · parameters of $\Phi_{T,\epsilon}$ 3.

$$\mathbb{Z}^r \xrightarrow{\kappa_2} T(\mathbb{Q}_p)_\epsilon \xrightarrow{\sim} \mathbb{Z}_p^{g+p-1}$$

$\cap$ dense

$\mathbb{Z}_p^r$

$\exists!\ \kappa = (\kappa_1, \dots, \kappa_{g+p-1})$

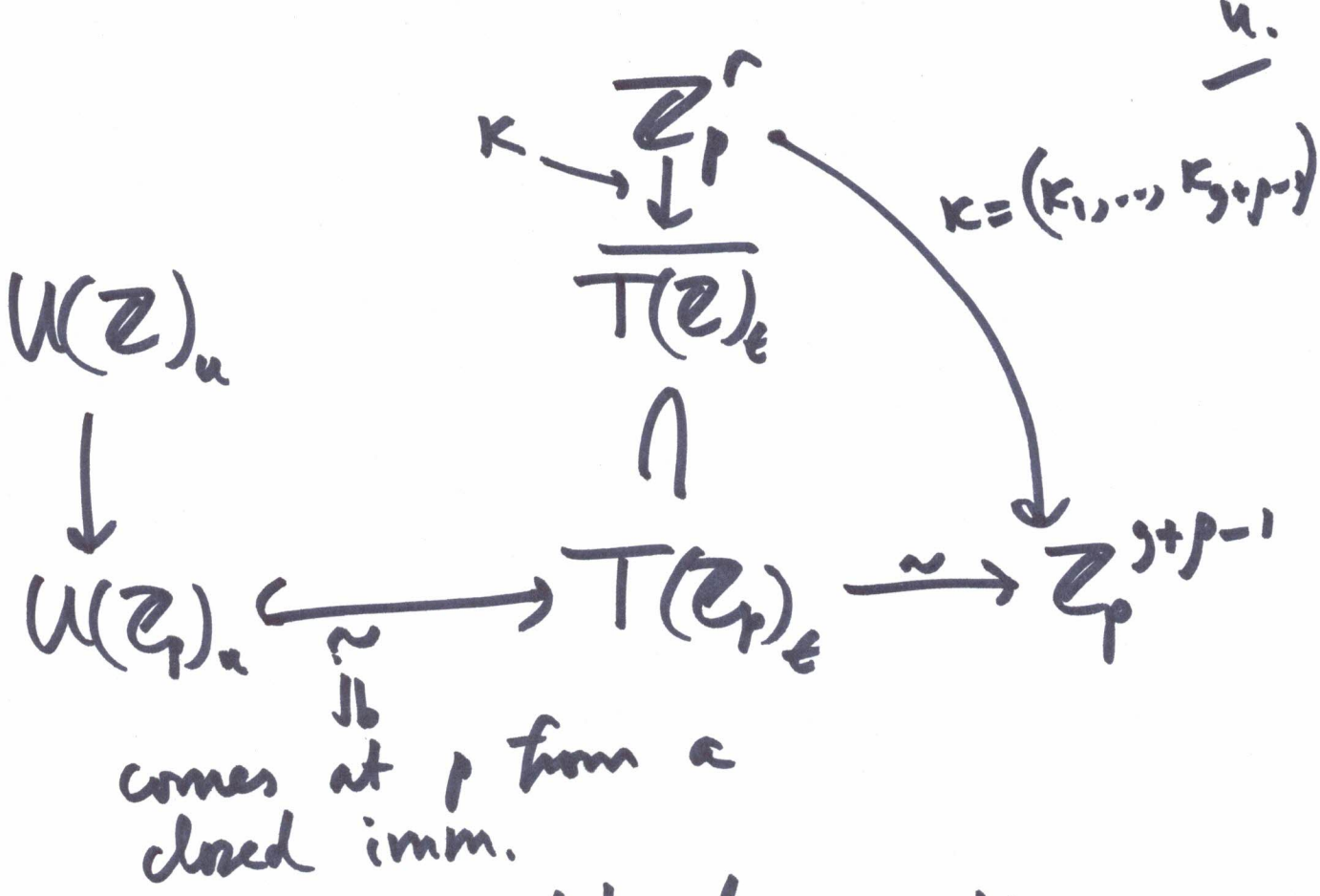
$\kappa_i \in \mathbb{Z}_p\langle\langle z_1, \dots, z_r\rangle\rangle$

$= \mathbb{Z}_p[z_1, \dots, z_r]^\wedge_p$

and $\overline{T(\mathbb{Q})_\epsilon}$ = image of κ.

Proof: all of §5, 3.5 pages logs & exp.

$n \in \mathbb{Z} \longmapsto n \cdot P = \exp(n \cdot \log P)$



1. we want to pull back equations for the complete int. $U \hookrightarrow T$ at u get $g+p-2$ equations to $\mathbb{Q}_p^r$.

2. We want to do this in terms of formal geometry, rings like $\mathbb{Q}_p\langle z_1, \dots z_r \rangle$, and then reduce mod p, get polynomials in $\mathbb{F}_p[z_1, \dots, z_r]$

Lecture 3: §3 & Thm. 4.12.

§3. p any prime number.

X smooth $\mathbb{Z}_p$-scheme, rel. dim. d

$x \in X(\mathbb{F}_p)$

$$\begin{array}{ccc} X(\mathbb{Z}_p) & \longrightarrow & X(\mathbb{F}_p) \\ \cup & & \cup \\ X(\mathbb{Z}_p)_x & \longrightarrow & \{x\} \end{array}$$

Let $p, t_1, \dots, t_d$ gen. of max. id. in $\mathcal{O}_{X,x}$.

$$X(\mathbb{Z}_p)_x \xrightarrow[\sim]{t_1,\dots,t_d} p\mathbb{Z}_p^d \xrightarrow[\sim]{\frac{1}{p}\cdot} \mathbb{Z}_p^d$$

$$\tilde{t} := (\tilde{t}_1, \dots, \tilde{t}_d) = \left(\frac{t_1}{p}, \frac{t_2}{p}, \dots, \frac{t_d}{p}\right)$$

Geometry. shrink X, s.t. it is affine, ϵ_i regular.

and $\epsilon: X \xrightarrow{\text{etale}} \mathbb{A}^d_{\mathbb{Z}_p}$ $\qquad \epsilon^{-1}\{p, \mathbb{F}_1\} = \{x\}$.

$\mathbb{Z}_p[\epsilon_1, \dots, \epsilon_d]$ $\qquad \epsilon_i$

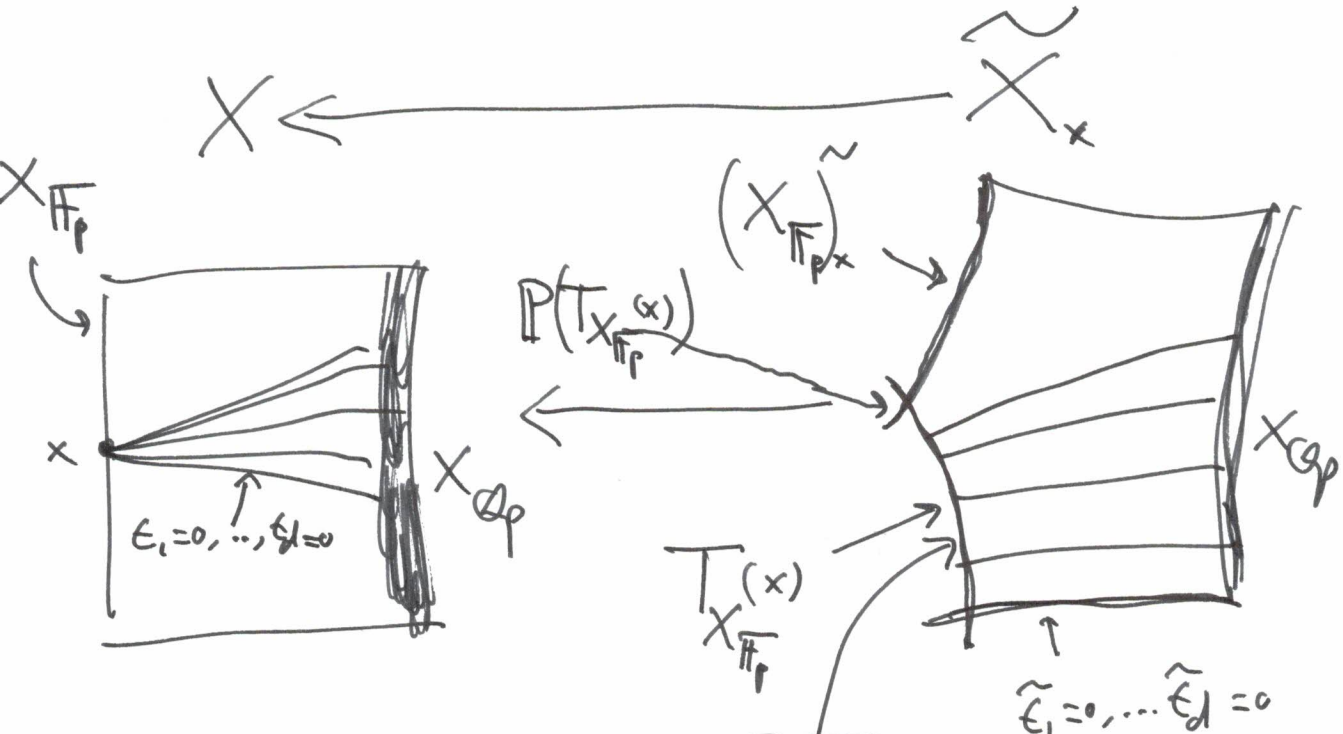
blow up in x:

$$\begin{array}{ccc} \tilde{X} & \xrightarrow{L} & \tilde{\mathbb{A}}^d_{\mathbb{Z}_p} \\ \pi \uparrow & & \uparrow \\ \tilde{X}_x & \longrightarrow & \tilde{\mathbb{A}}^d_{\mathbb{Z}_p,0} \\ \cup & & \uparrow \\ \tilde{X}^p_x & \xrightarrow{L} & \mathbb{A}^d_{\mathbb{Z}_p} \end{array} \qquad \bullet p$$

$p \cdot \tilde{\epsilon}_i$

$\mathbb{Z}_p[\tilde{\epsilon}_1, \dots, \tilde{\epsilon}_d]$ $\qquad \tilde{\epsilon}_i = \frac{\epsilon_i}{p}$.

Picture ("$d=1$, $p=5$")



complete along this part., complete padically.

This gives: $\mathbb{Z}_p\langle \tilde{\epsilon}_1, \dots, \tilde{\epsilon}_d \rangle = \mathbb{Z}_p[\tilde{\epsilon}_1, \dots, \tilde{\epsilon}_d]^{\wedge_p}$

$\mathcal{O}(\tilde{X}^p_x)^{\wedge_p} =$

$$\mathbb{F}_p \otimes_{\mathbb{Z}_p} \left(\mathcal{O}\left(\widetilde{X}^{\mathcal{P}}_{x} \right)^{\wedge_p} \right) = \mathbb{F}_p[\tilde{\xi}_1, \cdots, \tilde{\xi}_d].$$

geom: $T_{X_{\mathbb{F}_p}}(x)$. $p > 2$.

here we want $p \nmid n$ (good red. at p)

On Theorem 4.12.

Situation:

(affine) linear embedding of ardim. $g+p-2$

tangent map of j_b at u.

$$\mathbb{F}_p \otimes \mathcal{O}\left(\widetilde{T}^{\mathcal{P}}_{t}\right)^{\wedge_p} \ni \bar{f}_1, \cdots, \bar{f}_{g+p-2}$$

$T_{U_{\mathbb{F}_p}}(u)$

$$\begin{array}{ccc}
\left(\widetilde{U}^{\mathcal{P}}_{u}\right)_{\mathbb{F}_p} & \longrightarrow & \left(\widetilde{T}^{\mathcal{P}}_{t}\right)_{\mathbb{F}_p} \\
\downarrow & & \downarrow \\
\widetilde{U}^{\mathcal{P}}_{u} & \longrightarrow & \widetilde{T}^{\mathcal{P}}_{t} \\
\downarrow & & \downarrow \\
U & \xrightarrow{\tilde{j}_b} & T
\end{array}$$

$$\mathcal{U}(\mathbb{F}_p) \ni u \longmapsto t$$

$$\begin{array}{ccccc}
\mathcal{O}\left(\widetilde{U}^{\mathcal{P}}_{u}\right)^{\wedge_p} & \twoheadleftarrow & \mathcal{O}\left(\widetilde{T}^{\mathcal{P}}_{t}\right)^{\wedge_p} & \twoheadleftarrow & (f_1, \cdots, f_{g+p-2}) \\
 & & \downarrow k^* & & \downarrow (k^* f_i)_i \\
A & \twoheadleftarrow & \mathbb{Z}_p\langle z_1, \cdots, z_r \rangle & \twoheadleftarrow & I \\
\downarrow & & \downarrow & & \downarrow \\
\bar{A} & \twoheadleftarrow & \mathbb{F}_p[z_1, \cdots, z_r] & \twoheadleftarrow & \bar{I}
\end{array}$$

Thm. 4.12: $\overline{f_1}, \dots, \overline{f_{g+p-2}}$: deg ≤ 1.

$f_1, \dots, f_{g-1} \in \mathcal{O}_{J, j_b(u)}$

$\kappa^* \overline{f_1}, \dots, \kappa^* \overline{f_{g-1}}$: deg ≤ 1.

$\kappa^* \overline{f_g}, \dots, \kappa^* f_{g+p-2}$: deg ≤ 2.

One can compute the $\kappa^* \overline{f_i}$ in terms of $\mathbb{F}_p^r \xrightarrow{\overline{\kappa}} T(\mathbb{Z}/p^2\mathbb{Z})$

If $\overline{A}$ is finite, then $\dim_{\mathbb{F}_p}(\overline{A}) \geq \# U(\mathbb{Z})_u$.

Proof: A is p-adically complete. ☒

A is a f.g. $\mathbb{Z}_p$-module

Hence $\operatorname{rank}_{\mathbb{Z}_p}(A_{red}) \leq \dim_{\mathbb{F}_p}(\overline{A})$

$\leq \#\operatorname{Hom}_{\mathbb{Z}_p}(A_{red}, \mathbb{Z}_p)$

$= \#(U(\mathbb{Z})_u)$

Lecture 4. ① $\mathbb{Z}_p^r \xrightarrow{\kappa} T(\mathbb{Q}_p)_t$ $\quad r \leq g+p-2$.

$\uparrow \wr$ J_b

$U(\mathbb{Q}_p)_u$

Question: how can we prove, without doing computations, that $\kappa(\mathbb{Z}_p^r) \cap U(\mathbb{Q}_p)_u$ is finite? This should follow from our choice of $\mathcal{L}_1, \dots, \mathcal{L}_{p-1}$ on J, namely that they are $\mathbb{Z}$-lin. ind. in $NS(J_{\mathbb{Q}})$.

---

② $A^r_{\mathbb{F}_p} \xrightarrow{\bar{\kappa}} T_{T_{\mathbb{F}_p}}(t)$ can be non-injective,

for example if $p=1$, $J=T$, and

$$J(\mathbb{Z})_{0_{\mathbb{F}_p}} = \ker\left(J(\mathbb{Z}) \to J(\mathbb{Z}/p^2\mathbb{Z})\right). \quad (\text{then } \bar{\kappa}=0).$$

Two aims. ① Show that $\overline{A}$ as in Thm 4.12 can be computed, i.e. make it explicit.

② Show that the computations are not so bad.

①: §6–7.

§6. "Rigidify line bundles on C at b".

$$\mathrm{Pic}_{C/S}(T) = \frac{\mathrm{Pic}(C_T)}{\mathrm{Pic}(T)} =$$

$C \to S$ ($\mathbb{Z}[1/n]$)

$$= \{(\mathcal{L}, \varphi) : \mathcal{L} \text{ inv. } \mathcal{O}_{C_T}\text{-module on } C_T,\ \varphi : \mathcal{O}_T \xrightarrow{\sim} b_T^* \mathcal{L}\} / \cong$$

such objects have no nontrivial automorphisms.

Prop. 6.3.2 S any scheme, $C \to S$ proper smooth curve, of genus $g \geq 1$, $b \in C(S)$, $d \in \mathbb{Z}_{\geq 0}$.

$\exists!$ morphisms of $\mathbb{G}_m$-torsors, compatible with rigidif.'ns:

$$\begin{array}{ccccccc}
\mathcal{L}^{univ,\times} & \longrightarrow & P^\times & \longleftarrow & M^\times & \longleftarrow & N_d^\times \longleftarrow ?? \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
C \times_S J & \longrightarrow & J \times_S J^\vee & \xleftarrow{\sim} & J \times_S J & \xleftarrow[id \times \Sigma]{} & J \times_S C^{(d)} \\
 & & {\scriptstyle j_b \times j_b^{\vee,-1}} & & {\scriptstyle id \times j_b^{\vee,-1}} & & \uparrow \\
 & & & & & & \text{mod. space} \to C^d/S_d \\
 & & & & & & \text{of eff. div. degree } d \text{ on } C/S.
\end{array}$$

with: $N_d := Norm_{D_J^{univ}/J \times_S C^{(d)}}\left(\mathcal{L}^{univ}_{C^{(d)}}\right)$

$\mathcal{L}^{univ}_{C^{(d)}}$

where: $D^{univ} \to C \times C^{(d)}$, $D_J^{univ} \to C \times_S J \times_S C^{(d)}$

$D^{univ} \to C^{(d)}$ finite loc. free of degree d.

$C \times_S J \times_S C^{(d)} \to J \times_S C^{(d)}$

For example (6.3.12)

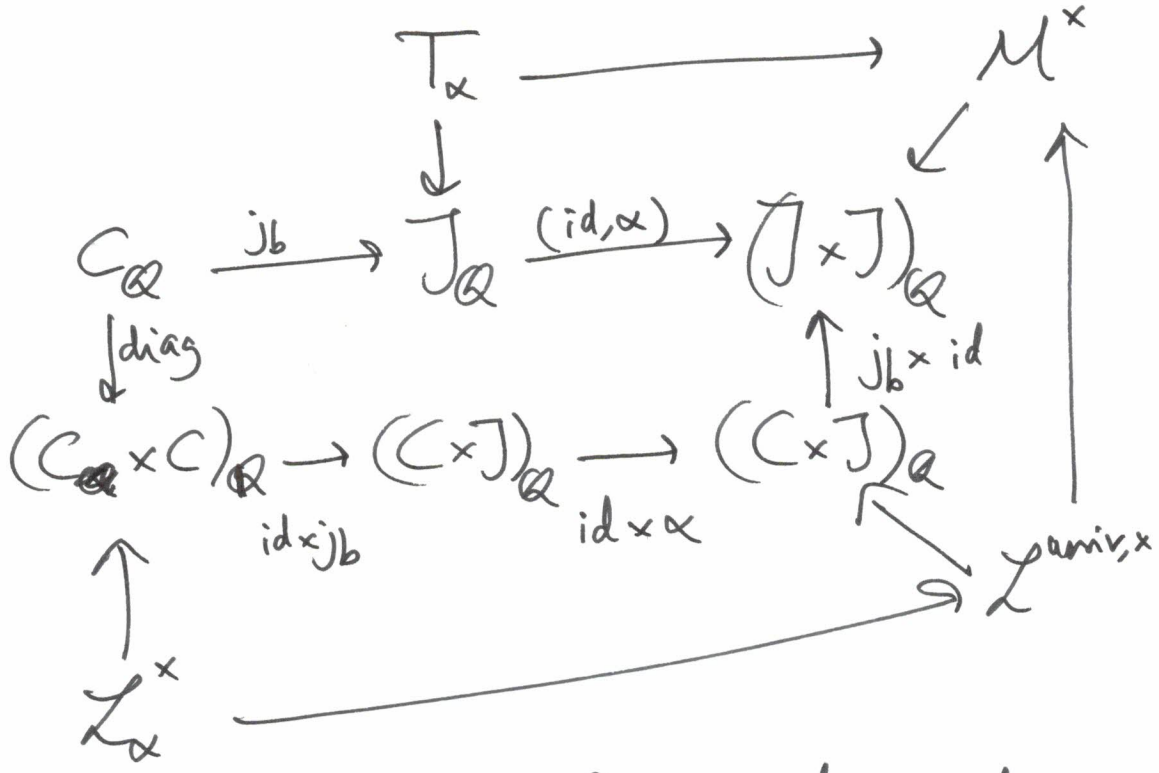
$x_i, y_i, u_j, v_j \in C(S)$

$$M\left(\sum_i (x_i - y_i), \sum_j (u_j - v_j)\right) =$$

$$= \bigotimes_j \left(u_j^* \mathcal{O}_C\left(\sum_i (x_i - y_i)\right) \otimes_{\mathcal{O}_S} v_j^* \mathcal{O}_C\left(\sum_i (y_i - x_i)\right)\right)$$

---

§7. $\alpha := tr_{b_i} \circ f_i : J_Q \to J_Q$; make explicit.



$j_b^* T_\alpha$ trivial on C_Q $\iff$ $\mathcal{L}_\alpha$ trivial on diagonal in $(C\times C)_Q$.

Computations in $T(\mathbb{Z}/p^2\mathbb{Z})$, $J(\mathbb{Z}/p^2\mathbb{Z})$, $J(\mathbb{F}_p)$.

1. $J(\mathbb{Z}/p^2\mathbb{Z})$, $J(\mathbb{F}_p)$: line bundles up to isom. on $C_{\mathbb{Z}/p^2\mathbb{Z}}$ or $C_{\mathbb{F}_p}$., e.g. work with divisors.

2. $T(\mathbb{Z}/p^2\mathbb{Z})$: no extra effort if you use rigidified line bundles.

Finally we get back to J, good or bad?

Compare with $Gr_{2g,g}$ Grassmannian of g-dim. subsp. in a 2g dim. space.

dim:  g^2.

embedded in: $\mathbb{P}^{\binom{2g}{g}-1}$ $\binom{2g}{g} \geq \frac{2^{2g}}{2g+1}$.

Not a problem: just describe subspaces by giving a basis.

Now J. Just the same.

Fix $\mathcal{L}$ on C of degree $\geq 3g-1$.

Then $\forall\ D \geq 0$ eff. div. degree g

$$H^0(C, \mathcal{L}(-D)) \hookrightarrow H^0(C, \mathcal{L})$$

is a codim. g subspace.

Details: Kamal Khuri-Makdisi
Peter Brün
implem. by Nicolas Mascot.