

Notes d'exposé.

Courbes lisses munies d'un gros  $p$ -groupe d'automorphismes en caractéristique  $p > 0$ , courbes maximales, courbes supersingulières.

1) Introduction

Notations:  $k$  corps alg. clos de car.  $p \geq 0$

$C/k$  courbe projective lisse connexe - genre  $g \geq 2$ .

$G$  sous-groupe de  $\text{Aut}_k(C)$

a) car(k) = 0  $|\text{Aut}_k(C)| \leq 84(g-1)$  (Hurwitz)

Problème: classification de ces groupes

Réponses partielles: • groupes d'Hurwitz (cf Conder 1990)

• groupes dits "larges", i.e.  $|G| \geq 4(g-1)$

(Kulbarni 97 - Breuer 00)

Principe: La formule de Riemann-Hurwitz impose des restrictions sur la ramification de  $C \rightarrow C/G$  ( $g_{C/G} = 0$ , lieu de ramification ---)

b) car(k) = p > 0  $|\text{Aut}_k(C)| \leq 16g^4$  (Stichtenoth 1973)

sauf  $W^q + W = X^{1+q}$ ,  $q = p^n \geq 3$

NB: apparition de "gros" groupes d'automorphismes due à la ramification sauvage.

c) Grosses actions:

Def:  $(C, G)$  est dite "grosse action" si

- \*  $G \subset \text{Aut}_k(C)$  avec  $G$   $p$ -groupe.
- \*  $|G| > \frac{2p}{p-1} g$ .

Prop: Soit  $(C, G)$  une grosse action. Soit  $\pi: C \rightarrow C/G$ .

- 1)  $\exists ! P \in C$  tel que  $P$  soit ramifié. Prenons  $P = \infty$ .
  - 2)  $\forall i \geq -1$ , soit  $G_i = i$ ème groupe de ramification inf. de  $G$  à l' $\infty$ .
- Alors,  $G = G_{-1} = G_0 = G_1 \supsetneq G_2 \neq \{e\}$

3)

$$\begin{array}{c}
 C \\
 \left| \begin{array}{c} G_2 \\ C/G_2 \simeq \mathbb{P}_R^1 \\ G/G_2 \simeq \{X \mapsto X+y, y \in V\} \\ C/G \simeq \mathbb{P}_R^1 \end{array} \right. \\
 G
 \end{array}$$

$$C/G_2 - \{\infty\} = \text{Spec } k[x]$$

$$\text{avec } 0 \longrightarrow G_2 \longrightarrow G \xrightarrow{\pi} V \simeq (\mathbb{Z}/p\mathbb{Z})^r \longrightarrow 0$$

$$\left[ \begin{array}{l} \text{à } \pi \left\{ \begin{array}{l} G \longrightarrow V \\ g \longmapsto g(x) - x \end{array} \right. \end{array} \right.$$

Preuve: formules de Riemann-Hurwitz et Riemann-Shafarevich.

2) Exemples en lien avec les courbes avec beaucoup de points rationnels.

Notations:  $k = \mathbb{F}_q$ ,  $q = p^n$ ,  $K = \mathbb{F}_q(X)$ ,  $m \in \mathbb{N}$

Def: (M. Perret, K. Lauter, R. Auer).

$K^m \subset K$  alg extension abélienne maximale  $L/K$

• de conducteur  $\leq m$  no

• telle que toute place  $(X-y)$ ,  $y \in \mathbb{F}_q$ , se décompose totalement dans  $L$

$C_m$  courbe telle que  $K(C_m) = K^m$

NB: existence et unicité de  $K^m$  dues à la théorie des corps de classe.

Prop:

1) Par unicité et maximalité de  $K^m$ , le groupe  $\{X \mapsto X+y, y \in \mathbb{F}_q\}$  se prolonge en un  $p$ -groupe  $G_m \subset \text{Aut}_k(C_m)$  tel que:

$$0 \longrightarrow \text{Gal}(K^m/K) \longrightarrow G_m \longrightarrow \mathbb{F}_q \longrightarrow 0$$

2) Pour  $n$  et  $m$  assez grands,  $(C_m, G_m)$  est une gross action avec  $(G_m)_2 = \text{Gal}(K^m/K)$ .

NB:  $\text{Gal}(K^m/K)$   $p$ -groupe abélien fini décrit par K. Lauter. (99).

Rem:  $N_m := |C_m(\mathbb{F}_q)| = 1 + q |\text{Gal}(K^m/K)| = 1 + |G_m|$ .

$$\text{D'ailleurs, } \frac{|G_m|}{q} \sim \frac{|N_m|}{q}$$

Lien entre courbes avec beaucoup de points rationnels et courbes avec un gros groupe d'automorphismes.

### 3) Grosses actions avec $G_2 \cong \mathbb{Z}/p\mathbb{Z}$

#### a) Paramétrisation

Théorème [C. Lehr, M. Malignon, 2005]

Soit  $(C, G)$  une grosse action avec  $G_2 \cong \mathbb{Z}/p\mathbb{Z}$ . Alors,

1)  $C \sim C_S : W^p - W = X S(X) \in k[X]$

où  $S(X) = (a_0 \text{id} + a_1 F + \dots + F^s)(X)$  additif de degré  $p^s$ ,  $s \geq 1$ . ( $F = \text{Frobenius}$ )

2) Soit  $\text{Ad}_S := F^s \left( \sum_{j=0}^s a_j F^j + F^{-j} a_j \right)$  polynôme palindromique de  $S$ . (cf Elkus 93)

Soit  $A_{p,s,1}$  le sous-groupe d'inertie sauvage de  $\text{Aut}_k(C)$  à l'is. Alors,

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & A_{p,s,1} & \longrightarrow & \mathbb{Z}(\text{Ad}_S) \cong (\mathbb{Z}/p\mathbb{Z})^{2s} \longrightarrow 0 \\ & & \parallel & & \cup & & \cup \\ 0 & \longrightarrow & G_2 & \longrightarrow & G & \longrightarrow & \mathbb{V} \longrightarrow 0 \end{array}$$

(zéros de  $\text{Ad}_S$ )

Pour  $p \geq 3$ ,  $A_{p,s,1}$  est l'unique groupe extraspecial d'ordre  $p^{2s+1}$  et d'exposant  $p$ .

3) Réciproquement, si  $C_S : W^p - W = X S(X) \in k[X]$ ,  $S$  additif,  $(C_S, A_{p,s,1})$  est une grosse action avec un  $G_2 \cong \mathbb{Z}/p\mathbb{Z}$ .

Corollaire: Si  $(C, G)$  est une grosse action, alors  $G_2 = D(G)$  le groupe dérivé de  $G$ .

Preuve: taille maximale des sous-groupes abéliens normaux des groupes extraspecials.

NB: Comme  $G_2 \neq \{e\}$ ,  $G$  n'est pas abélien dans le cas d'une grosse action.

#### b) Optimalité des courbes: $W^p - W = X S(X) \in \mathbb{F}_q[X]$ , $S$ additif.

i) rappels:  $k = \mathbb{F}_q, q = p^n$

$C/k$  projective lisse géométriquement irréductible. genre:  $g$ .

$N_i := |C(\mathbb{F}_q^i)|$  nombre de points rationnels de  $C$  vue sur  $\mathbb{F}_q^i$ .

Fonction Zêta de  $C$ :  $\zeta(C, t) = \exp\left(\sum_{i=1}^{+\infty} \frac{N_i}{i} t^i\right)$  pour  $t \in \mathbb{C}, |t| < 1/q$ .

Thm:  $\zeta(C, t) = \frac{L(t)}{(1-t)(1-qt)}$  où  $L(t) \in \mathbb{Z}[t]$  polynôme de degré  $2g$ .

Si  $\zeta(C, t) = \prod_{i=1}^{2g} (1 - \omega_i t)$  avec  $\omega_i \in \mathbb{C}$ , alors  $N_n = 1 + q^n - \sum_{i=1}^{2g} \omega_i^n$ .

Bornes de Hasse-Weil:  $1 + q - 2g\sqrt{q} \leq |C(\mathbb{F}_q)| \leq 1 + q + 2g\sqrt{q}$ .

↑  
courbe dite  $\mathbb{F}_q$ -minimale

↑  
courbe dite  $\mathbb{F}_q$ -maximale

Thm:  $C$  est  $\mathbb{F}_q$ -maximale  $\Leftrightarrow \forall 1 \leq i \leq 2g, \omega_i = -\sqrt{q}$ .  
 $C$  est  $\mathbb{F}_q$ -minimale  $\Leftrightarrow \forall 1 \leq i \leq 2g, \omega_i = \sqrt{q}$ .

ii) cas des courbes:  $C: W^p - W = XS(X), S$  additif

Prop: Soit  $C: W^p - W = XS(X) \in \mathbb{F}_q[X], S$  additif.

[On suppose  $\mathbb{F}_q \supset \mathbb{Z}(A_d)$ . Alors,  $C$  est  $\mathbb{F}_q$ -maximale ou  $\mathbb{F}_q$ -minimale.

Idee de la preuve:  $\pi: C \rightarrow C/\langle \sigma \rangle \simeq \mathbb{P}_{\mathbb{F}_q}^1$  où  $\sigma: \begin{cases} X \rightarrow X \\ W \rightarrow W+1 \end{cases}$

revêtement galoisien d'ordre  $p$ , totalement ramifié à l'infini, étale au-dessus de la droite affine. On note  $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$  la fonction trace.

$$|C(\mathbb{F}_q)| = 1 + p \cdot \left| \left\{ y \in \mathbb{F}_q, \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(y S(y)) = 0 \right\} \right|$$

$\uparrow$   
 $\infty \in \mathbb{P}_{\mathbb{F}_q}^1$  est totalement ramifié

$\uparrow$   
 $y \in \mathbb{F}_q$  admet  $p$  points rationnels "au-dessus"  
 $\Leftrightarrow W^p - W - y S(y)$  admet une racine dans  $\mathbb{F}_q$

$$\Leftrightarrow \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(y S(y)) = 0 \quad (\text{Thm 50 de Hilbert})$$

On étudie les vecteurs isotropes de la forme quadratique  $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x S(x))$ .

On trouve  $|C(\mathbb{F}_q)| = 1 + q + 2 \varepsilon q \sqrt{q}$  où  $\varepsilon = \pm 1$  selon le discriminant de la forme quadratique.

d) supersingularité des courbes  $C: W^p - W = XS(X) \in \mathbb{k}[X], S$  additif

i) rappels:

Def:  $\mathbb{k}$  corps de car.  $p > 0$ .  $C/\mathbb{k}$  est dite supersingulière si  $\text{Jac}(C)$  est géométriquement isogène à un produit de courbes elliptiques supersingulières (i.e. sans point géométrique d'ordre  $p$ ).

Thm: Supposons  $C$  définie sur  $\mathbb{F}_q$ .

[ $C$  est supersingulière si et seulement si  $\exists k \in \mathbb{N}^*, \forall 1 \leq i \leq 2g, \omega_i^k = \pm q^{k/2}$ .

$\rightarrow$  Cor: Si  $C$  est  $\mathbb{F}_q$ -maximale ou  $\mathbb{F}_q$ -minimale,  $C$  est supersingulière.

Un autre critère...

Thm:  $C_1/\mathbb{k}$  et  $C_2/\mathbb{k}$  courbes projectives lisses géométriquement irréductibles.

On suppose qu'il existe un morphisme fini séparable  $C_1 \rightarrow C_2$ .

Alors la supersingularité de  $C_1$  implique celle de  $C_2$ .

ii) application aux courbes  $C: W^p - W = X S(X) \in k[X]$ ,  $S$  additif

Prop:  $k = \bar{k}$ , car  $(k) = p > 0$ .

$C: W^p - W = X S(X) \in k[X]$ ,  $S$  additif.

Alors,  $C$  est supersingulière.

Rem: énoncé prouvé dans le cas d'un corps fini par van der Geer, van der Vlugt (92).  
 on généralise ici au cas " $k$  alg. clos".

Éléments de preuve:

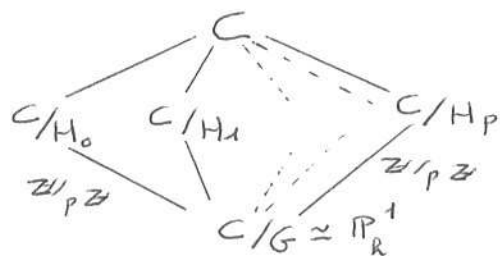
Supposons  $p \geq 3$  et  $S$  additif de degré  $p^s$ ,  $s \geq 1$ .

$A_{p,s,1}$  comme défini en a) est alors le groupe extraspecial d'ordre  $p^{2s+1}$  et d'exposant  $p$ .

Son centre  $Z(A_{p,s,1}) = \langle \sigma \rangle \cong \mathbb{Z}/p\mathbb{Z}$  où  $\sigma \begin{cases} X \mapsto X \\ W \mapsto W+1 \end{cases}$

Soit  $\tau \in A_{p,s,1} - Z(A_{p,s,1})$ .  $\tau$  est d'ordre  $p$  et  $G := \langle \sigma, \tau \rangle \cong (\mathbb{Z}/p\mathbb{Z})^2$ .

$G$  admet  $(p+1)$  sous-groupes non triviaux (i.e. d'ordre  $p$ ):  $\begin{cases} H_i = \langle \sigma \tau^i \rangle, 0 \leq i \leq p-1 \\ H_p = \langle \tau \rangle. \end{cases}$



Par Garcia-Stichtenoth [91], comme  $g_{C/G} = 0$ ,

alors  $g_C = g_{C/H_0} + g_{C/H_1} + \dots + g_{C/H_p}$ .

Par Kani-Rosen [89] (Thm. C), comme  $H_i H_j = H_j H_i = G$ ,  $\forall i \neq j$ , et  $g(C/H_i H_j) = 0$ ,

$\text{Jac}(C) \sim_{\text{isogène}} \text{Jac}(C/H_0) \times \text{Jac}(C/H_1) \times \dots \times \text{Jac}(C/H_p)$ .

Or  $C/H_0 \cong \mathbb{P}^1_R$  et  $\forall i \geq 1$ ,  $C/H_i: v_i^p - v_i = u \sum_i (u)$  où  $\sum_i$  additif de degré  $p^{s-1}$ . (van der Geer 92)

Par une "récurrence descendante", on parvient à  $W^p - W = X^2$  (défini sur  $\mathbb{F}_q$ !) dont on sait qu'elle est soit  $\mathbb{F}_q$ -maximale, soit  $\mathbb{F}_q$ -minimale (voir c). C'est donc une courbe supersingulière.

4) Grosses actions avec  $G_2 \cong (\mathbb{Z}/p\mathbb{Z})^m$ ,  $m \geq 1$ .

a) Paramétrisation. (on tente de généraliser le cas  $G_2 \cong \mathbb{Z}/p\mathbb{Z}$ ).

Déf.  $t \geq 1$ . On définit  $Z_t$  comme le  $k$  sev de  $k[X]$  engendré par 1 et le produit d'au plus  $t$  polynômes additifs.

Caractérisation:

1)  $a \in \mathbb{N}$  avec  $a = a_0 + a_1 p + \dots + a_\ell p^\ell$  où  $0 \leq a_i \leq p-1$ .

Alors  $X^a \in Z_t \iff S_p(a) := a_0 + a_1 + \dots + a_\ell \leq t$ .

2)  $f(X) = \sum_{a \in \mathbb{N}} c_a(f) X^a \in k[X] - \{0\}$

Alors,  $f(X) \in Z_t \iff \forall a \in \mathbb{N}$  avec  $c_a(f) \neq 0$ ,  $S_p(a) \leq t$ .

Thm: [Rocher 09]

Soit  $(C, G)$  une grosse action avec  $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$ ,  $n \geq 1$ .

Saent  $L := h(C)$  et  $h(X) = LG_2$ .

Alas il existe un système d'équations  $L(h(X): W_i^p - W_i = f_i(X) \in h[X]$ ,  $1 \leq i \leq m$  avec chaque  $f_i$  dans  $Z_{i+1}$ .

Preuve: voir thèse - chapitre 3.

NB: 1) par ce système de fonctions  $f_i$ :  
$$\forall 1 \leq i \leq m, \forall y \in V, f_i(x+y) = f_i(x) + \sum_{j=1}^{i-1} \underbrace{h_j(y)}_{\in \mathbb{F}_p} f_j(x) \pmod{(F-id)(h[X])}$$

i.e. le système d'équations est globalement stable par translation par  $V$ . (système "triangulaire")

• 2) généralisation du cas  $n=1$  à  $f(X) = XS(X) \in Z_2$ .

• 3) pour  $n \geq 2$ , la réciproque n'est plus vraie.

Un cas particulier...

Thm [Rocher 09]

Soit  $(C, G)$  une grosse action avec  $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$ ,  $n \geq 2$  et  $\forall 1 \leq i \leq m, f_i \in Z_{i+1} - Z_i$ .

Alas,  $n \leq p-1$ ,  $\dim_{\mathbb{F}_p} V = 1+s$  et  $\forall 1 \leq i \leq m, \deg |f_i| = 1+ip^s$ .

Preuve: voir thèse - chapitre 3.

NB: Ce théorème est suffisamment précis pour donner un algorithme de paramétrisation de la famille universelle correspondante pour  $p$  et  $s$  assez petits.

Voir illustrations ci-jointes pour  $p=5, s=1$ .

## PARAMETRISATION POUR $p = 5, s = 1, n = 2$ .

### • Paramétrisation:

$$f_1(X) = X^6 + 2(b^{25} + b)b^{-5}X^2 = X S_1(X)$$

$$f_2(X) = b^5 X^{11} + 4b^{25} X^7 + 2(b^{50} - b^2)b^{-5} X^3 + cX$$

avec  $b \in k^\times$  et  $c \in k$  algébriquement indépendants.

$$V = Z(\text{Ad}_{S_1}) = Z(X^{25} + 4(b^{125} + b^5)b^{-25}X^5 + X)$$

### • Courbes isomorphes:

$C(b, c) \sim C(b', c')$  si et seulement si:

$$\left(\frac{b'}{b}\right)^{24} = 1 \quad \text{et} \quad c' = \lambda \frac{b'}{b} c \quad \text{avec} \quad \lambda \in \mathbb{F}_5^\times.$$

### • Description de $G$ :

1.  $G$  est d'ordre  $5^4$ , d'exposant 5 et de 5-rang 2.
2.  $Z(G)$  est cyclique d'ordre 5.
3.  $G/Z(G)$  est extraspécial d'exposant 5.
4. Soit  $C_G(G_2)$  le centralisateur de  $G_2$  dans  $G$ .

$$C_G(G_2) \simeq (\mathbb{Z}/5\mathbb{Z})^3 \supsetneq G_2 \simeq (\mathbb{Z}/5\mathbb{Z})^2.$$

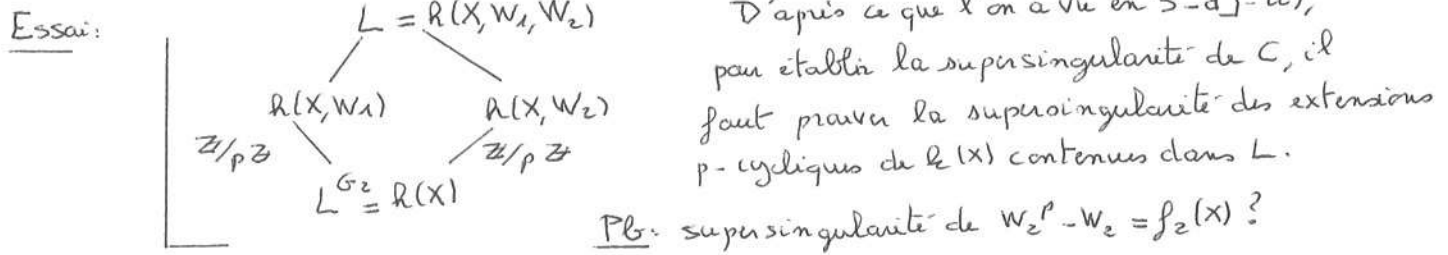
b) Discussion autour de la supersingularité de ces courbes.

i) Cas de la famille universelle paramétrée précédemment par  $p=5, s=1, m=2$ .

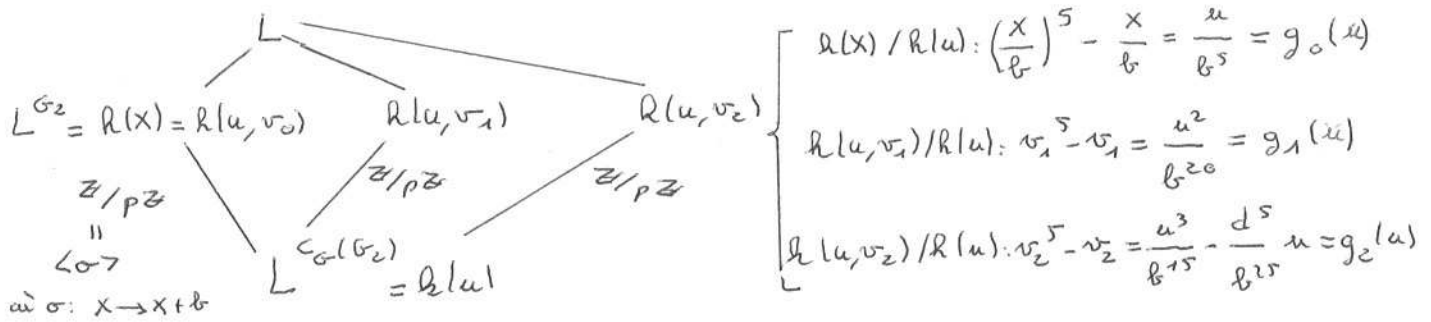
$$C: \begin{cases} W_1^p - W_1 = f_1(X) = X^6 + 2(b^{25} + b)b^{-5}X^2 = X S_1(X) \\ W_2^p - W_2 = f_2(X) = b^5 X^{11} + 4b^{25} X^7 + 2(b^{50} - b^2)b^{-5}X^3 + cX \end{cases} \quad (b, c) \in \mathbb{k}^x \times \mathbb{k}$$

$$L := \mathbb{k}(c) \text{ et } L^{G_2} = \mathbb{k}(X).$$

Idee: appliquer la technique utilisée pour  $C: W^p - W = X S(X)$  (voir 3) d-ii).



Essai plus fructueux: on considère le centralisateur de  $G_2$  dans  $G$ :  $C_G(G_2)$   
on montre qu'ici  $C_G(G_2) \cong (\mathbb{Z}/p\mathbb{Z})^3 \supsetneq G_2 \cong (\mathbb{Z}/p\mathbb{Z})^2$ .



On a trouvé 3 extensions  $p$ -cycliques de  $\mathbb{k}(u)$   $\mathbb{F}_p$ -indépendantes dont le compositum est  $L$ .  
 Les autres extensions  $p$ -cycliques de  $\mathbb{k}(u)$  sont données par:  $w^p - w = \lambda_0 g_0(u) + \lambda_1 g_1(u) + \lambda_2 g_2(u)$   
 où  $[\lambda_0, \lambda_1, \lambda_2] \in \mathbb{P}^2(\mathbb{F}_p)$ . Celle-ci est une sous-famille de la famille générale:  $\alpha u + \beta u^2 + \gamma u^3$   
 $(\alpha, \beta, \gamma) \in \mathbb{k}^3$ , laquelle est supersingulière pour  $p=5$ . (preuve: par translation, on peut prendre  $\beta=0$ . La courbe  $w^5 - w = \alpha u + \gamma u^3$  est alors vérifiée par  $w^5 - w = \alpha u^2 + \gamma u^6 = u S(u)$  supersingulière).

Conclusion: pour  $p=5, s=1, n=2$ , la courbe obtenue est supersingulière.

ii) Autres cas.

Même cas que précédemment  $s=1, n=2$  mais  $p \geq 7$ .

Mêmes équations en remplaçant 5 par  $p$ . On applique la méthode ci-dessus.

On est encore une fois ramené à discuter de la supersingularité de  $w^p - w = \alpha u + \beta u^2 + \gamma u^3$

$(\alpha, \beta, \gamma) \in \mathbb{k}^3$ . Mais pour  $p \geq 7$ , cette courbe n'est plus supersingulière.

→ preuve on utilise les travaux de Scholten et Zhu [Comp. 91] pour calculer la

première pente du polygone de Newton =  $NP_1(C)$

Pour  $p \geq 7$ , leur formule donne  $NP_1(C) = \frac{\Gamma(p-1)}{p-1} \neq 1/2$   $\square$ .