Formules de Thomae et isogénies

Romain COSSET

CNRS
Laboratoire: LORIA (Nancy), Équipe: CACAO

26 mars 2010

FONCTIONS THÊTA

Fonctions thêta analytiques

Ce sont des fonctions de $\mathbb{C}^g$ dans $\mathbb{C}$.

Soient $z \in \mathbb{C}^g$, $(a,b) \in \mathbb{Q}^{2g}$ et $\Omega \in \mathcal{H}_g$.

$$\begin{aligned}
\theta(z,\Omega) &= \sum_{n\in\mathbb{Z}^g} \exp\left(\pi i^t n\Omega n + 2\pi i^t n\cdot z\right) \\
\theta[a,b](z,\Omega) &= \sum_{n\in\mathbb{Z}^g} \exp\left(\pi i^t (n+a)\Omega(n+a) + 2\pi i^t (n+a)\cdot(z+b)\right) \\
&= \exp\left(\pi i^t a\Omega a + 2\pi i^t a\cdot(z+b)\right)\theta(z+\Omega a+b,\Omega)
\end{aligned}$$

(a,b) est appelé la caractéristique de la fonction thêta.

Nous allons considérer

- z modulo $\Lambda = \mathbb{Z}^g + \Omega\mathbb{Z}^g$.
- les caractéristiques (a,b) modulo $\mathbb{Z}^{2g}$.

Variétés abéliennes

Variété abélienne

C'est un groupe algébrique complet connexe.

Cad. une variété algébrique avec une loi de groupe algébrique.

Exemples de variétés abéliennes :

- les courbes elliptiques
- les jacobiennes de courbes.

Variétés abéliennes

Variété abélienne

C'est un groupe algébrique complet connexe.

Cad. une variété algébrique avec une loi de groupe algébrique.

Exemples de variétés abéliennes :

- les courbes elliptiques
- les jacobiennes de courbes.

Elles sont utilisées en cryptographie car

- Le problème du logarithme discret y est (souvent) difficile.
- Il y existe des couplages.

Variétés abéliennes

Une variété abélienne A de dimension g (principalement polarisée) est analytiquement isomorphe à $\mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ pour un certain $\Omega \in \mathcal{H}_g$.

Pour $n \geq 3$, la variété A se plonge dans $\mathbb{P}^{n^g-1}(\mathbb{C})$ à l'aide des fonctions thêta de niveau n.

Niveau d'une fonction thêta

- Niveau (n,n)

$$\theta\left[\frac{a}{n},\frac{b}{n}\right](nz,\Omega) \qquad \text{avec } a,b \in \mathbb{Z}^g$$

- Niveau n

$$\theta\left[0,\frac{b}{n}\right]\left(z,\frac{\Omega}{n}\right) \qquad \text{avec } b \in \mathbb{Z}^g$$

Niveau d'une fonction thêta

- Niveau (n,n)

$$\theta\left[\frac{a}{n},\frac{b}{n}\right](nz,\Omega) \qquad \text{avec } a,b\in\mathbb{Z}^g$$

- Niveau n

$$\theta\left[0,\frac{b}{n}\right]\left(z,\frac{\Omega}{n}\right) \qquad \text{avec } b\in\mathbb{Z}^g$$

Les fonctions thêta de niveau (n,n) et n^2 fournissent deux plongement isomorphes de la variété abélienne dans $\mathbb{P}^{n^{2g}-1}(\mathbb{C})$.

Niveau d'une fonction thêta

- Niveau (n,n)

$$\theta\left[\frac{a}{n},\frac{b}{n}\right](nz,\Omega) \qquad \text{avec } a,b\in\mathbb{Z}^g$$

- Niveau n

$$\theta\left[0,\frac{b}{n}\right]\left(z,\frac{\Omega}{n}\right) \qquad \text{avec } b\in\mathbb{Z}^g$$

Les fonctions thêta de niveau (n,n) et n^2 fournissent deux plongement isomorphes de la variété abélienne dans $\mathbb{P}^{n^{2g}-1}(\mathbb{C})$.

Arithmétique :

- Niveau $4=(2,2)$
- Niveau 2 : surface de Kummer $A/\{\pm 1\}$

Formules de Thomae

$$\mathrm{Jac}(\mathcal{C}) \xrightarrow{\sim} \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g) \hookrightarrow \mathbb{P}^{n^g-1}(\mathbb{C})$$

Formules de Thomae

Elles relient des puissances des thêta constantes avec les paramètres de la courbe.

Formules existantes :

- Courbes elliptiques et hyperelliptiques ; niveau $(2,2)$. (Thomae)
- Courbes elliptiques ; niveau $(3,3)$. (Thomae)
- ...

Formules de Thomae

$$\mathrm{Jac}(\mathcal{C}) \xrightarrow{\sim} \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g) \hookrightarrow \mathbb{P}^{n^g-1}(\mathbb{C})$$

Formules de Thomae

Elles relient des puissances des thêta constantes avec les paramètres de la courbe.

Formules existantes :

- Courbes elliptiques et hyperelliptiques ; niveau $(2,2)$. (Thomae)
- Courbes elliptiques ; niveau $(3,3)$. (Thomae)
- ...

Exemple pour la courbe $\mathcal{E}$: $y^2 = x(x-1)(x-\lambda)$:

$$\left(\frac{\theta\left[0,\frac{1}{2}\right](0)}{\theta[0,0](0)}\right)^4 = 1 - \frac{1}{\lambda} \qquad \left(\frac{\theta\left[\frac{1}{2},0\right](0)}{\theta[0,0](0)}\right)^4 = \lambda$$

GÉNÉRALISATION DES FORMULES DE THOMAE

Cas du genre 1

Soit une courbe elliptique sur un corps K quelconque.

Outils :

- Surfaces de Riemann
- Couplage de Tate

Étant donnée la r-torsion sur la courbe elliptique, on obtient les thêta constantes de niveau (r,r) à la puissance $r' = 2\,\mathrm{ppcm}(2,r)$.

Cas du genre 1

Soit une courbe elliptique sur un corps K quelconque.

Outils :

- Surfaces de Riemann
- Couplage de Tate

Étant donnée la r-torsion sur la courbe elliptique, on obtient les thêta constantes de niveau (r,r) à la puissance $r' = 2\,\mathrm{ppcm}(2,r)$.

Programme magma :
ENTRÉE : Une courbe elliptique, un point de r-torsion correspondant à $a\tau + b$.
SORTIE : La thêta constante $\theta[a,b](0,\tau)^{r'}$

Exemple en genre 1

Soit $\mathcal{C} : y^2 = x(x-1)(x-\lambda)$ associée à $\tau_\lambda \in \mathcal{H}$: $\mathcal{C}(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z} + \tau_\lambda \mathbb{Z})$.

Points de 2-torsion :

$$\infty \leftrightsquigarrow 0 \qquad (0,0) \leftrightsquigarrow \tau_\lambda/2 \qquad (1,0) \leftrightsquigarrow 1/2 \qquad (\lambda,0) \leftrightsquigarrow 1/2 + \tau_\lambda/2$$

Exemple en genre 1

Soit $\mathcal{C} : y^2 = x(x-1)(x-\lambda)$ associée à $\tau_\lambda \in \mathcal{H}$: $\mathcal{C}(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z} + \tau_\lambda \mathbb{Z})$.

Points de 2-torsion :

$$\infty \leftrightsquigarrow 0 \qquad (0,0) \leftrightsquigarrow \tau_\lambda/2 \qquad (1,0) \leftrightsquigarrow 1/2 \qquad (\lambda,0) \leftrightsquigarrow 1/2 + \tau_\lambda/2$$

Soit $P = (x_0, y_0)$ de 6-torsion tel que $3 * P = (0,0)$.
Supposons que P s'envoie sur le point $\tau_\lambda/6$, alors

$$\left(\frac{\theta[1/6,0](0)}{\theta(0)}\right)^{12} = \frac{\lambda-1}{4}x_0^3 + \frac{3\lambda-2}{16}x_0^2 + \frac{-12\lambda^2+13\lambda-2}{8}x_0 + \dots$$

$$\left(\frac{\theta[2/6,0](0)}{\theta(0)}\right)^{12} = \frac{-\lambda+1}{4\lambda}x_0^3 + \frac{-2\lambda+3}{16}x_0^2 + \frac{-2\lambda^2+13\lambda-12}{8}x_0 + \dots$$

$$\left(\frac{\theta[3/6,0](0)}{\theta(0)}\right)^{12} = \lambda^3$$

Cas du genre ≥ 2

En genre ≥ 2, la méthode précédente (basée sur les surfaces de Riemann) ne marche pas.

Cas du genre ≥ 2

En genre ≥ 2, la méthode précédente (basée sur les surfaces de Riemann) ne marche pas.

Pour tout $a, b \in \mathbb{Z}^g$ et tout $\alpha, \beta \in \mathbb{Z}^g$,

$$\theta\left[\frac{a}{n}, \frac{b}{n}\right]\left(\Omega\frac{\alpha}{r} + \frac{\beta}{r}, \Omega\right) = \omega\,\theta\left[\frac{a}{n} + \frac{\alpha}{r}, \frac{b}{n} + \frac{\beta}{r}\right](0, \Omega)$$

Soit P un point de r-torsion dont on connaît les coordonnées par les fonctions thêta de niveau (n, n). On a alors les thêta constantes de niveau (nr, nr).

Cas du genre ≥ 2

En genre ≥ 2, la méthode précédente (basée sur les surfaces de Riemann) ne marche pas.

Pour tout $a, b \in \mathbb{Z}^g$ et tout $\alpha, \beta \in \mathbb{Z}^g$,

$$\theta\left[\frac{a}{n}, \frac{b}{n}\right]\left(\Omega\frac{\alpha}{r} + \frac{\beta}{r}, \Omega\right) = \omega\, \theta\left[\frac{a}{n} + \frac{\alpha}{r}, \frac{b}{n} + \frac{\beta}{r}\right](0, \Omega)$$

Soit P un point de r-torsion dont on connaît les coordonnées par les fonctions thêta de niveau (n, n). On a alors les thêta constantes de niveau (nr, nr).

La variété abélienne $A = \mathrm{Jac}(\mathcal{C})$ se plonge dans $\mathbb{P}^{n^{2g}-1}$ grâce aux fonctions thêta de niveau (n, n).
On trouve $P = \left[\quad \theta\left[\frac{a}{n}, \frac{b}{n}\right](z_P, \Omega)\right]_{a,b \in \mathbb{Z}^g}$ un point de r-torsion.

Cas du genre ≥ 2

En genre ≥ 2, la méthode précédente (basée sur les surfaces de Riemann) ne marche pas.

Pour tout $a, b \in \mathbb{Z}^g$ et tout $\alpha, \beta \in \mathbb{Z}^g$,

$$\theta\left[\frac{a}{n}, \frac{b}{n}\right]\left(\Omega\frac{\alpha}{r} + \frac{\beta}{r}, \Omega\right) = \omega\, \theta\left[\frac{a}{n} + \frac{\alpha}{r}, \frac{b}{n} + \frac{\beta}{r}\right](0, \Omega)$$

Soit P un point de r-torsion dont on connaît les coordonnées par les fonctions thêta de niveau (n, n). On a alors les thêta constantes de niveau (nr, nr).

La variété abélienne $A = \mathrm{Jac}(\mathcal{C})$ se plonge dans $\mathbb{P}^{n^{2g}-1}$ grâce aux fonctions thêta de niveau (n, n).
On trouve $P = \left[\lambda_P \theta\left[\frac{a}{n}, \frac{b}{n}\right](z_P, \Omega)\right]_{a,b \in \mathbb{Z}^g}$ un point de r-torsion.

On doit calculer λ_P.

Facteur projectif λ_P

Grâce aux formules d'addition (affine) on peut calculer

- λ_P^r pour r impair.
- λ_P^{2r} pour r pair.

On obtient les $\theta\left[\frac{a}{r},\frac{b}{r}\right](0,\Omega)^{2r}$ avec $a,b \in \mathbb{Z}^g$.
On a des formules à la Thomae pour le niveau (r,r).

Extraction de racines

Étude de l'action des sous groupes de $\mathrm{Sp}(2g,\mathbb{Z})$ sur $\mathbb{C}^g \times \mathcal{H}_g$

Les formules de Thomae fournissent les puissances quatrièmes des thêta constantes de niveau $(2,2)$.
On peut extraire ces racines (quitte à prendre un isomorphisme).

- genre 1 : **ok**.
- genre 2 : **ok** mais utilisation des formules de Frobenius...
- genre ≥ 3 : Ok pour certaines et les carrés des autres.

De même il est possible d'obtenir les thêta constantes de niveaux $(2r,2r)$ en genre 1 et 2 pour r impair.

Descente de niveau

Supposons donnée les thêta constantes de niveau ln, on veut obtenir les thêta constantes de niveau n :

$$\theta\left[0,\frac{b}{ln}\right]\left(0,\frac{\Omega}{ln}\right) \longrightarrow \theta\left[0,\frac{b'}{n}\right]\left(0,\frac{\Omega}{n}\right)$$

Application aux formules de Thomae :

Si on a les thêta constantes de niveau $n^2 = (n,n)$, on obtient celle de niveau n.

Formule de Koizumi

Formule de Koizumi

Exprime $\prod_{i=1}^{m} \theta\left[K_1^{(i)}, K_2^{(i)}\right]\left(Z^{(i)}, \gamma_i \Omega\right)$ en fonction d'une somme de $\prod_{i=1}^{m} \theta\left[L_1^{(i)} + P_1^{(i)}, L_2^{(i)} + P_2^{(i)}\right]\left(W^{(i)}, \delta_i \Omega\right)$

Formule de Koizumi

Soient $\Gamma = \mathrm{diag}(\gamma_1, \ldots, \gamma_m)$ et $\Delta = \mathrm{diag}(\delta_1, \ldots, \delta_m)$ avec $\gamma_i, \delta_i \in \mathbb{Q}_+^*$.

Soient $K_1, K_2 \in \mathrm{M}_{g\times m}(\mathbb{Q})$ des caractéristiques pour m fonctions thêta.
Soient $L_1, L_2 \in \mathrm{M}_{g\times m}(\mathbb{Q})$ des caractéristiques pour m fonctions thêta.
Soient $Z \in \mathrm{M}_{g\times m}(\mathbb{C})$ et $W \in \mathrm{M}_{g\times m}(\mathbb{C})$ des variables pour m fonctions thêta.

Formule de Koizumi

Exprime $\prod_{i=1}^m \theta\left[K_1^{(i)}, K_2^{(i)}\right]\left(Z^{(i)}, \gamma_i\Omega\right)$ en fonction d'une somme de
$\prod_{i=1}^m \theta\left[L_1^{(i)} + P_1^{(i)}, L_2^{(i)} + P_2^{(i)}\right]\left(W^{(i)}, \delta_i\Omega\right)$

Formule de Koizumi

Soient $\Gamma = \mathrm{diag}(\gamma_1, \ldots, \gamma_m)$ et $\Delta = \mathrm{diag}(\delta_1, \ldots, \delta_m)$ avec $\gamma_i, \delta_i \in \mathbb{Q}_+^*$.
Supposons qu'il existe $T \in \mathrm{GL}_m(\mathbb{Q})$ tel que ${}^tT\Gamma T = \Delta$.
Soient $K_1, K_2 \in \mathrm{M}_{g\times m}(\mathbb{Q})$ des caractéristiques pour m fonctions thêta.
Soient $L_1, L_2 \in \mathrm{M}_{g\times m}(\mathbb{Q})$ telles que $L_1 = K_1 {}^tT^{-1}$, $L_2 = K_2 T$.
Soient $Z \in \mathrm{M}_{g\times m}(\mathbb{C})$ et $W \in \mathrm{M}_{g\times m}(\mathbb{C})$ avec $W = ZT$.

Formule de Koizumi

Exprime $\prod_{i=1}^m \theta\left[K_1^{(i)}, K_2^{(i)}\right]\left(Z^{(i)}, \gamma_i\Omega\right)$ en fonction d'une somme de
$\prod_{i=1}^m \theta\left[L_1^{(i)} + P_1^{(i)}, L_2^{(i)} + P_2^{(i)}\right]\left(W^{(i)}, \delta_i\Omega\right)$
avec $P_1 \in M {}^tT^{-1}/\left(M \cap M {}^tT^{-1}\right)$ et $P_2 \in MT/(M \cap MT)$ où $M = \mathrm{M}_{g\times m}(\mathbb{Z})$.

Applications de la formule de Koizumi

La formule de Koizumi contient :

- Formules de Riemann
- Équivalence entre le niveau (n,n) et le niveau n^2.
- Formules d'additions
- ...

Applications de la formule de Koizumi

La formule de Koizumi contient :

- Formules de Riemann
- Équivalence entre le niveau (n,n) et le niveau n^2.
- Formules d'additions
- ...

On veut du niveau n à partir du niveau n^2.
Pour avoir du Ω/n et du Ω/n^2 on prend $\Gamma = \frac{1}{n}\mathrm{Id}_m$ et $\Delta = \frac{1}{n^2}\mathrm{Id}_m$.
On cherche une matrice $T \in \mathrm{GL}_m(\mathbb{Q})$ telle que

$$ {}^tT \left(\frac{1}{n}\mathrm{Id}_m\right) T = \frac{1}{n^2}\mathrm{Id}_m $$

C'est à dire telle que

$$ {}^tTT = \frac{1}{n}\mathrm{Id}_m $$

Choix de la matrice T

Choix de la matrice T telle que ${}^tTT = \frac{1}{n}\mathrm{Id}_m$

- Pour $n = a^2$, $T = [\frac{1}{a}]$
- Pour $n = a^2 + b^2$, $T = \frac{1}{n}\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ (multiplication par $(a+ib)^{-1}$).
- Pour $n = a^2 + b^2 + c^2 + d^2$, matrice de la multiplication par $(a + ib + jc + kd)^{-1}$ dans la base $(1, i, j, k)$.

Choix de la matrice T

Choix de la matrice T telle que ${}^tTT = \frac{1}{n}\mathrm{Id}_m$

- Pour $n = a^2$, $T = [\frac{1}{a}]$
- Pour $n = a^2 + b^2$, $T = \frac{1}{n}\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ (multiplication par $(a+ib)^{-1}$).
- Pour $n = a^2 + b^2 + c^2 + d^2$, matrice de la multiplication par $(a+ib+jc+kd)^{-1}$ dans la base $(1, i, j, k)$.

Pour tout entier n, on obtient une matrice T (non unique).
Soit $n \in \mathbb{N}$, quelle est la dimension minimale m de T ?

- si $m = 1$ alors n est un carré.
- si $m = 2$ alors n est somme de deux carrés
- si $m = 3$ alors n est somme de trois carrés et n'est pas premier.

Algorithme

ENTRÉE : Une courbe hyperelliptique $\mathcal{C}$ de genre $g = 2$ donnée sous forme de Weierstrass et un niveau $r \in \mathbb{N}$.
SORTIE : Les thêta constantes de niveau r.

1. Calcul des puissances des thêta de niveau $(2,2)$.
2. Extraire les racines.
3. Calcul de la r-torsion dans $\mathrm{Jac}(\mathcal{C})$.
4. Obtenir la r-torsion exprimée avec les fonctions thêta de niveau $(2,2)$.
5. Calcul des puissances thêta de niveau (r,r).
6. Extraire les racines.
7. Descendre de niveau.

ISOGÉNIES

Comment prendre des isogénies

On s'interesse à des ℓ-isogénies pour ℓ premier impair.

On utilise les fonctions thêta de niveau $n\ell$ avec $n = 2$ ou 4.

Comment prendre des isogénies

On s'interesse à des ℓ-isogénies pour ℓ premier impair.
On utilise les fonctions thêta de niveau $n\ell$ avec $n = 2$ ou 4.

Pour avoir une ℓ-isogénie, on peut

- oublier des coordonnées (descente de niveau) :

$$\theta\left[0, \frac{b}{\ell n}\right]\left(0, \frac{\Omega}{\ell n}\right) \xrightarrow{\pi} \theta\left[0, \frac{b'}{n}\right]\left(0, \frac{\Omega}{\ell n}\right) = \theta\left[0, \frac{b'}{n}\right]\left(0, \frac{\Omega/\ell}{n}\right)$$

- prendre l'isogénie duale (montée de niveau).

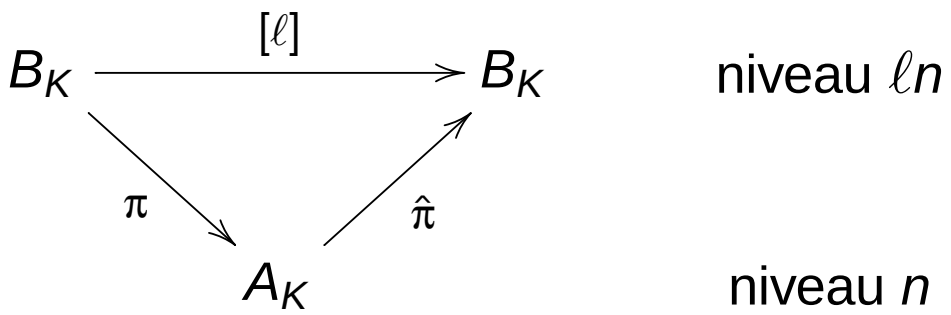


Diagramme commutatif

Avec les formules de Koizumi, on peut descendre de niveau sans prendre d'isogénie :

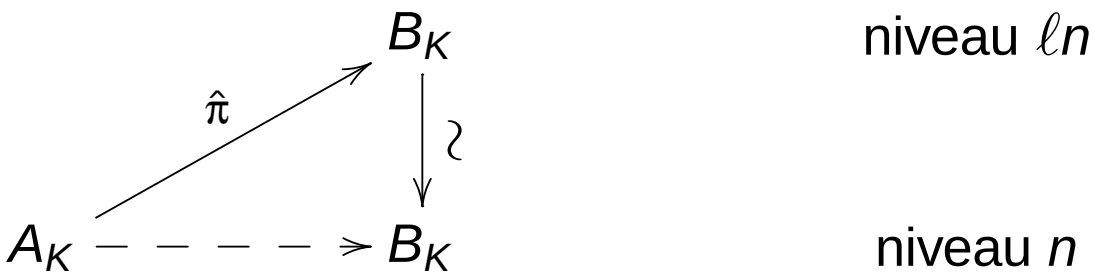
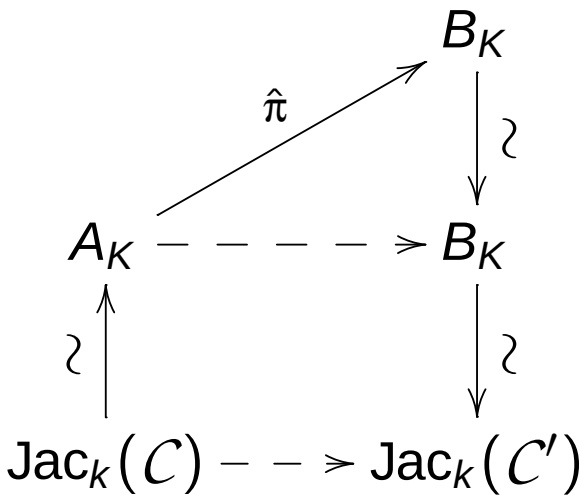


Diagramme commutatif

Avec les formules de Koizumi, on peut descendre de niveau sans prendre d'isogénie .
Attention : pour des courbes définies sur un corps, il faut en général prendre une extension de corps K/k pour utiliser les thêta constantes.

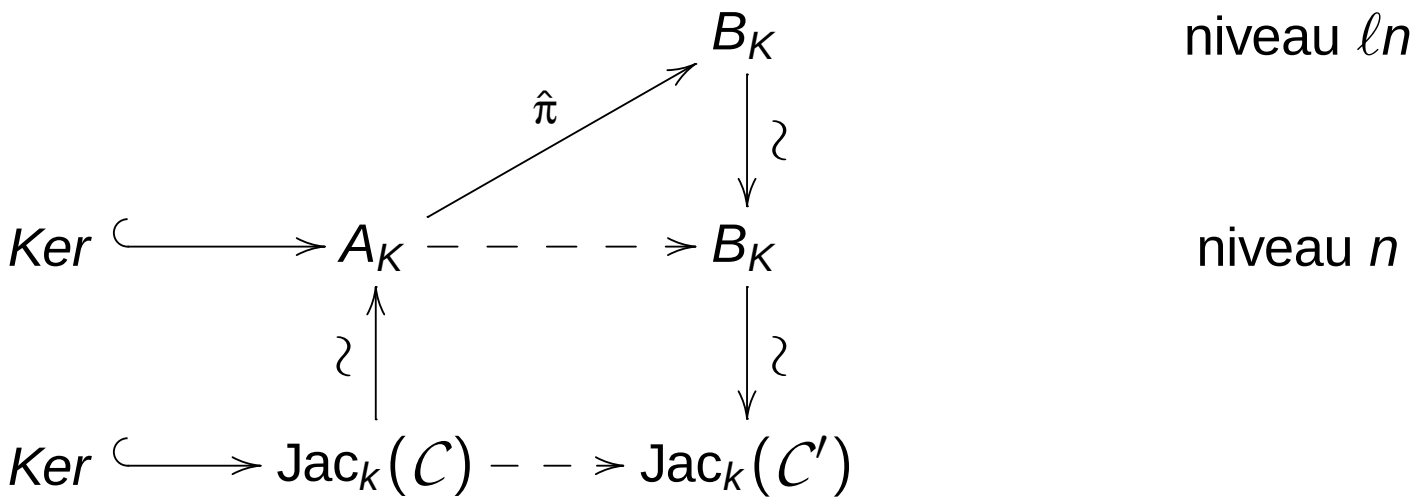


niveau ℓn

niveau n

Diagramme commutatif

Avec les formules de Koizumi, on peut descendre de niveau sans prendre d'isogénie .
Attention : pour des courbes définies sur un corps, il faut en général prendre une extension de corps K/k pour utiliser les thêta constantes.
L'isogénie est définie par son noyau Ker. Il est plus facile de prouver la rationnalité de ce dernier du côté de la jacobienne.



En pratique

- On utilise $n = 2$ ou 4.
- On a plusieurs choix de racines à faire.
- La courbe finale $\mathcal{C}'$ est sur K/k et doit être transformée en une courbe rationnelle sur k.
- Expression de l'isomorphisme $\mathrm{Jac}_k(\mathcal{C}) \xrightarrow{\sim} A_K$: OK pour $g = 1, 2, 3$.

En pratique

- On utilise $n = 2$ ou 4.
- On a plusieurs choix de racines à faire.
- La courbe finale $\mathcal{C}'$ est sur K/k et doit être transformée en une courbe rationnelle sur k.
- Expression de l'isomorphisme $\mathrm{Jac}_k(\mathcal{C}) \xrightarrow{\sim} A_K$: OK pour $g = 1, 2, 3$.

- Programme magma : en cours.

- Complexité : calcul de la ℓ-torsion.

Conclusion

Résultats obtenus

- On obtient des formules à la Thomae pour
  - Genre 1, niveau quelconque.
  - Genre 2, niveau quelconque.
  - Genre ≥ 3, niveau (r,r) si on connait le niveau $(2,2)$.
  - Genre ≥ 3, niveau r si on connait le niveau (r,r).

- On peut prendre des ℓ-isogénies sans changer de niveau.

Travaux futurs

- Finir de programmer les algorithmes.
- Étudier leur complexité.

- Continuer à étudier l'action des sous-groupes $\mathrm{Sp}(2g)$.
- Genre $g \geq 3$.