Algèbres d'invariants pour les courbes hyperelliptiques de genre 3 en caractéristiques positives

Romain Basson

IRMAR - Université de Rennes 1

Journées C2, Grenoble
24 mars 2014

Notations

- k un coprs et $\overline{k}$ une clôture algébrique de k ;
- espace des formes binaires de degré n à coefficients dans k :

$$V_n(k) = \left\{ \sum_{i=0}^{n} a_i x^i z^{n-i} \ / \ a_i \in k \right\};$$

- $\mathrm{GL}_2(\overline{k})$ agit sur $V_n(\overline{k})$, pour $f \in V_n(\overline{k})$ et $M \in \mathrm{GL}_2(\overline{k})$:

$$(M.f)(x,z) = f(M.(x,z)), \quad \forall (x,z) \in \overline{k}^2.$$

Courbes elliptiques

On suppose $\mathrm{char}\, k \neq 2, 3$.

- Les courbes elliptiques $E/k : y^2 = x^3 + ax + b$ sont classifiées à $\overline{k}$-isomorphisme près par

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2};$$

- Pour $j \in \overline{k} \setminus \{1728\}$, la courbe elliptique E suivante vérifie $j(E) = j$:

$$E/k(j) : y^2 = x^3 - \frac{27j}{j - 1728} x + \frac{54j}{j - 1728};$$

- $$Aut(E) \simeq \begin{cases} C_2 & \text{si } j(E) \neq 0, 1728 \\ C_4 & \text{si } j(E) = 1728 \\ C_6 & \text{si } j(E) = 0 \end{cases}.$$

Courbes hyperellitpiques

On suppose dorénavant char $k \neq 2$.

Problème

Peut-on faire la même chose pour les courbes hyperelliptiques de genre $g \geqslant 2$, i.e. $C/k : y^2 = f(x)$, où $\deg f = 2g + 2$ et f est séparable ?

$$\{\text{Courbes hyperelliptiques de genre } g\}_{/\simeq} \longleftrightarrow \{\text{espace de paramètres}\}$$

Courbes hyperellitpiques

On suppose dorénavant char $k \neq 2$.

Problème

Peut-on faire la même chose pour les courbes hyperelliptiques de genre $g \geqslant 2$, i.e. $C/k : y^2 = f(x)$, où $\deg f = 2g + 2$ et f est séparable ?

$$\{\text{Courbes hyperelliptiques de genre } g\}_{/\simeq} \longleftrightarrow \{\text{espace de paramètres}\}$$

Motivations :

- tester "arithmétiquement" si deux courbes sont isomorphes ;
- reconnaître le groupe d'automorphismes d'une courbe ;
- obtenir des informations géométriques et arithmétiques sur l'espace de module ;
- énumérer les courbes sur un corps finis pour des expérimentations.

Courbes hyperelliptiques *vs* Formes binaires

On se place dans l'espace projectif pondéré $\mathbb{P}(1, 1, g+1)$.

Proposition

Soit $C : y^2 = f(x, z)$ et $C' : y^2 = f'(x, z)$ deux courbes hyperelliptiques de genre g. Tout isomorphisme de C sur C' est de la forme :

$$(x : z : y) \longmapsto (ax + bz : cx + dz : ey)$$

où $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\overline{k})$ *et* $e \in \overline{k}^\star$.

Courbes hyperelliptiques *vs* Formes binaires

On se place dans l'espace projectif pondéré $\mathbb{P}(1, 1, g+1)$.

Proposition

Soit $C : y^2 = f(x, z)$ et $C' : y^2 = f'(x, z)$ deux courbes hyperelliptiques de genre g. Tout isomorphisme de C sur C' est de la forme :

$$(x : z : y) \longmapsto (ax + bz : cx + dz : ey)$$

où $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\overline{k})$ *et* $e \in \overline{k}^\star$.

Le problème de la classification à isomorphisme près des courbes hyperelliptiques de genre g se réduit ainsi à celui de l'équivalence de deux formes binaires sous l'action de $\mathrm{GL}_2(\overline{k})$.

Algèbres d'invariants de formes binaires

On note $\mathcal{I}_n(k) = \overline{k}[V_n]^{\mathrm{GL}_2(\overline{k})}$ l'algèbre graduée (par le degré) des invariants des formes binaires de degré n sous l'action de $\mathrm{GL}_2(\overline{k})$.

Exemple : le discriminant de $f \in V_n$ est un invariant de degré $2n-2$.

Algèbres d'invariants de formes binaires

On note $\mathcal{I}_n(k) = \overline{k}[V_n]^{\mathrm{GL}_2(\overline{k})}$ l'algèbre graduée (par le degré) des invariants des formes binaires de degré n sous l'action de $\mathrm{GL}_2(\overline{k})$.

Exemple : le discriminant de $f \in V_n$ est un invariant de degré $2n-2$.

Proposition

Soit f et $f' \in V_n(k)$, avec $n \geqslant 3$, dont les multiplicités des racines (dans $\overline{k}$) sont $< n/2$. $GL_2(\overline{k}).f = GL_2(\overline{k}).f'$ si et seulement s'il existe $\lambda \in \overline{k}$ tel que $J(f) = \lambda^d J(f')$, pour tout $J \in \mathcal{I}_n$ homogène de degré d.

Algèbres d'invariants de formes binaires

On note $\mathcal{I}_n(k) = \overline{k}[V_n]^{\mathrm{GL}_2(\overline{k})}$ l'algèbre graduée (par le degré) des invariants des formes binaires de degré n sous l'action de $\mathrm{GL}_2(\overline{k})$.

Exemple : le discriminant de $f \in V_n$ est un invariant de degré $2n-2$.

Proposition

Soit f et $f' \in V_n(k)$, avec $n \geqslant 3$, dont les multiplicités des racines (dans $\overline{k}$) sont $< n/2$. $GL_2(\overline{k}).f = GL_2(\overline{k}).f'$ si et seulement s'il existe $\lambda \in \overline{k}$ tel que $J(f) = \lambda^d J(f')$, pour tout $J \in \mathcal{I}_n$ homogène de degré d.

Théorème (Gordan, 1868, $k = \mathbb{C}$)

$\mathcal{I}_n(\mathbb{C})$ est une $\mathbb{C}$-algèbre de type fini.

- La preuve de Gordan est effective ;
- le théorème de Gordan reste valable pour l'action d'un groupe réductif, comme $\mathrm{GL}_2(\overline{k})$.

Générateurs de $\mathcal{I}_n$

Il s'agit donc de déterminer des générateurs de $\mathcal{I}_n$, ce qui était déjà une question classique au XIX$^{\text{ème}}$ siècle pour $k = \mathbb{C}$:

- $n \leqslant 6$: connu depuis le XIX$^{\text{ème}}$;
- $n = 7$: von Gall (1888) et Dixmier et Lazard (1986) ;
- $n = 8$: von Gall (1880) et Shioda (1967) ;
- $n = 9, 10$: Brouwer et Popoviciu (2009, 2010).

Générateurs de $\mathcal{I}_n$

Il s'agit donc de déterminer des générateurs de $\mathcal{I}_n$, ce qui était déjà une question classique au XIX$^{\text{ème}}$ siècle pour $k = \mathbb{C}$:

- $n \leqslant 6$: connu depuis le XIX$^{\text{ème}}$;
- $n = 7$: von Gall (1888) et Dixmier et Lazard (1986) ;
- $n = 8$: von Gall (1880) et Shioda (1967) ;
- $n = 9, 10$: Brouwer et Popoviciu (2009, 2010).

Stratégie mise en œuvre :

- trouver un système homogène de paramètres , *i.e.* des invariants primaires ;
- utiliser la série de Hilbert de $\mathcal{I}_n$ pour déterminer des invariants secondaires.

Les séries de Hilbert de $\mathcal{I}_n(\mathbb{C})$, pour $n \leqslant 10$, ont été données par Sylvester et Franklin (1879).

Corps de caractéristique positive

Théorème (Geyer, 1974)

Si k est un corps de caractéristique $p > n$, alors

$$\mathcal{I}_n(k) = \mathcal{I}_n(\mathbb{Z}[1/n!]) \otimes k.$$

Corps de caractéristique positive

Théorème (Geyer, 1974)

Si k est un corps de caractéristique $p > n$, alors

$$\mathcal{I}_n(k) = \mathcal{I}_n(\mathbb{Z}[1/n!]) \otimes k.$$

- Genre 2 : invariants d'Igusa définis sur $\mathbb{Z}$ (1960).

Corps de caractéristique positive

Théorème (Geyer, 1974)

Si k est un corps de caractéristique $p > n$, alors

$$\mathcal{I}_n(k) = \mathcal{I}_n(\mathbb{Z}[1/n!]) \otimes k.$$

- Genre 2 : invariants d'Igusa définis sur $\mathbb{Z}$ (1960).
- Genre 3 :
  - Lercier, Ritzenthaler : extension des résultats de Shioda pour $p > 7$;

Corps de caractéristique positive

Théorème (Geyer, 1974)

Si k est un corps de caractéristique $p > n$, alors

$$\mathcal{I}_n(k) = \mathcal{I}_n(\mathbb{Z}[1/n!]) \otimes k.$$

- Genre 2 : invariants d'Igusa définis sur $\mathbb{Z}$ (1960).
- Genre 3 :
  - Lercier, Ritzenthaler : extension des résultats de Shioda pour $p > 7$;
  - pas de résultat pour $p \in \{3, 5, 7\}$.

Corps de caractéristique positive

Théorème (Geyer, 1974)

Si k est un corps de caractéristique $p > n$, alors

$$\mathcal{I}_n(k) = \mathcal{I}_n(\mathbb{Z}[1/n!]) \otimes k.$$

- Genre 2 : invariants d'Igusa définis sur $\mathbb{Z}$ (1960).
- Genre 3 :
  - Lercier, Ritzenthaler : extension des résultats de Shioda pour $p > 7$;
  - pas de résultat pour $p \in \{3, 5, 7\}$.

Difficulté : les séries de Hilbert ne sont pas connues pour ces derniers cas.

Corps de caractéristique 3

$\mathcal{I}_8(k) = k[J_2, \ldots, J_{10}]$, lorsque car $k > 7$.

Corps de caractéristique 3

$\mathcal{I}_8(k) = k[J_2, \ldots, J_{10}]$, lorsque car $k > 7$.

Lorsque car $k = 3$, on peut calculer 10 invariants linéairement indépendants : $J_2, \ldots, J_{10}, J_{12}$.

Question : $\mathcal{I}_8(k) = k[J_2, \ldots, J_{10}, J_{12}]$?

Corps de caractéristique 3

$\mathcal{I}_8(k) = k[J_2, \ldots, J_{10}]$, lorsque car $k > 7$.

Lorsque car $k = 3$, on peut calculer 10 invariants linéairement indépendants : $J_2, \ldots, J_{10}, J_{12}$.

Question : $\mathcal{I}_8(k) = k[J_2, \ldots, J_{10}, J_{12}]$?

Question alternative : ces 10 invariants permettent-ils de classifier à isomorphisme près les courbes hyperelliptiques de genre 3 définies sur k ?

Invariants diédraux

$$W = \left\{ \sum_{i=1}^{8} a_i x^i z^{8-i} \in V_8(\overline{k}) \ / \ a_1 = a_7 = 0 \right\} < V_8(\overline{k}).$$

$$D = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} / \lambda, \mu \in \overline{k}^\star \right\rangle \subset \mathrm{GL}_2(\overline{k}) \text{ agit sur } \overline{k}[V_8] \text{ et } \overline{k}[W].$$

Invariants diédraux

$$W = \left\{ \sum_{i=1}^{8} a_i x^i z^{8-i} \in V_8(\overline{k}) \ / \ a_1 = a_7 = 0 \right\} < V_8(\overline{k}).$$

$$D = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} / \lambda, \mu \in \overline{k}^\star \right\rangle \subset \mathrm{GL}_2(\overline{k}) \text{ agit sur } \overline{k}[V_8] \text{ et } \overline{k}[W].$$

$\overline{k}[V_8]^D$ admet un système de 20 générateurs.

$\overline{k}[W]^D = k[i_1, i_2, k_2, l_2, j_3, l_3, i_4, j_5]$, où

$$i_1 = a_4,\ i_2 = a_0 a_8,\ k_2 = a_2 a_6,\ l_2 = a_3 a_5, \ldots$$

qui satisfont les deux relations :

$$\mathfrak{R}_1 = 2 i_4 l_3 + j_3 l_2^2 + j_5 k_2 \text{ et } \mathfrak{R}_2 = 2 i_4^2 + j_5 j_3 + 2 l_3^2 i_2 + l_2^2 k_2 i_2.$$

$\mathcal{I}_8 = \overline{k}[V_8]^{\mathrm{GL}\,2(\overline{k})} \subset \overline{k}[V_8]^D$, ainsi les invariants de Shioda s'expriment à partir des invariants diédraux :

- $J_2 = 2i_1^2 + i_2 + j_2 + k_2 + l_2$;
- $J_3 = 2i_1 i_2 + i_1 k_2 + i_3 + 2k_3$;
- $J_4 = i_1^4 + 2i_1^2 i_2 + i_1^2 j_2 + j_2^2 + 2i_1^2 k_2 + i_2 k_2 + i_1^2 l_2 + j_2 l_2 + l_2^2 + 2i_1 i_3 + 2i_1 k_3 + 2i_4 + 2k_4$;
- $J_5 = i_1^5 + 2i_1^3 i_2 + i_1^3 j_2 + i_1 j_2^2 + i_1 i_2 k_2 + 2i_1 j_2 k_2 + 2i_1 k_2^2 + 2i_1^3 l_2 + 2i_1 i_2 l_2 + i_1 k_2 l_2 + 2i_1^2 i_3 + 2k_2 i_3 + l_2 i_3 + i_1^2 j_3 + 2k_2 j_3 + 2l_2 j_3 + i_1^2 k_3 + j_2 k_3 + k_2 k_3 + 2l_2 k_3 + 2i_2 l_3 + 2j_2 l_3 + k_2 l_3 + l_2 l_3 + i_1 j_4 + 2i_1 k_4 + i_1 l_4 + 2i_1 m4 + j_5 + k_5 + l_5$;
- ...

Reconstruction pour W

À $f \in W$ est associé un point $(i_1(f) : i_2(f) : \ldots : j_5(f))$.

Reconstruction pour W

À $f \in W$ est associé un point $(i_1(f) : i_2(f) : \ldots : j_5(f))$.

Réciproquement, étant donné un point $(i_1 : i_2 : \ldots : j_5) \in \mathbb{P}(1, 2, 2, 2, 3, 3, 4, 5)$, satisfaisant $\mathfrak{R}_1$ et $\mathfrak{R}_2$, on sait déterminer $f \in W$ telle que

$$(i_1(f) : i_2(f) : \ldots : j_5(f)) = (i_1 : i_2 : \ldots : j_5).$$

Reconstruction pour W

À $f \in W$ est associé un point $(i_1(f) : i_2(f) : \ldots : j_5(f))$.

Réciproquement, étant donné un point $(i_1 : i_2 : \ldots : j_5) \in \mathbb{P}(1, 2, 2, 2, 3, 3, 4, 5)$, satisfaisant $\mathfrak{R}_1$ et $\mathfrak{R}_2$, on sait déterminer $f \in W$ telle que

$$(i_1(f) : i_2(f) : \ldots : j_5(f)) = (i_1 : i_2 : \ldots : j_5).$$

Par exemple, si $k_2 = 0$ and $j_3, l_3 \neq 0$, on peut choisir

$$f = \frac{i_2}{l_3^2 j_3} x^8 + \frac{1}{l_3} x^6 + \frac{l_2}{l_3} x^5 + i_1 x^4 + l_3 x^3 + l_3^2 j_3.$$

Preuve : on vérifie, via un système de calcul formel, que la forme reconstruite a des invariants diédraux égaux à $(i_1 : i_2 : \ldots : j_5)$.

Des invariants de Shioda aux invariants diédraux

Il reste à savoir déterminer les invariants diédraux $i_1, i_2, \ldots, j_5$ à partir des invariants de Shioda $J_2, \ldots, J_{10}, J_{12}$.

Des invariants de Shioda aux invariants diédraux

Il reste à savoir déterminer les invariants diédraux $i_1, i_2, \ldots, j_5$ à partir des invariants de Shioda $J_2, \ldots, J_{10}, J_{12}$.

Génériquement :

- i_1 est n'importe quelle racine de :

$$0 = X^{13} + 2J_3 X^{10} + \cdots + 2J_3 J_5^2 + 2J_3 J_{10} \ ;$$

- les 7 autres invariants $i_2, \ldots, j_5$ sont solutions d'équations linéaires.

Il y a en outre quelques cas particuliers, lorsque les coefficients dominants s'annulent.

Des invariants de Shioda aux invariants diédraux

Il reste à savoir déterminer les invariants diédraux $i_1, i_2, \ldots, j_5$ à partir des invariants de Shioda $J_2, \ldots, J_{10}, J_{12}$.

Génériquement :

- i_1 est n'importe quelle racine de :

$$0 = X^{13} + 2J_3\,X^{10} + \cdots + 2J_3J_5^2 + 2J_3J_{10}\ ;$$

- les 7 autres invariants $i_2, \ldots, j_5$ sont solutions d'équations linéaires.

Il y a en outre quelques cas particuliers, lorsque les coefficients dominants s'annulent.

Comment expliquer cette ambiguïté sur i_1 ?

Des invariants de Shioda aux invariants diédraux

Les invariants diédraux sont plus grossiers que les invariants de Shioda, précisément

Proposition

Pour $f \in V_8$, avec $\mathrm{Disc}(f) \neq 0$, le cardinal de $(\mathrm{GL}_2(\overline{k}).f \cap W)/D$ est constant, égal à 13.

Des invariants de Shioda aux invariants diédraux

Les invariants diédraux sont plus grossiers que les invariants de Shioda, précisément

Proposition

Pour $f \in V_8$, avec $\mathrm{Disc}(f) \neq 0$, le cardinal de $(\mathrm{GL}_2(\overline{k}).f \cap W)/D$ est constant, égal à 13.

Lemme

Pour tout $f \in V_8$, il existe $g = \sum_{i=0}^{8} b_i x^i z^{8-i} \in \mathrm{GL}_2(\overline{k}).f$ telle que

$$\begin{cases} b_0 b_8 \neq 0 \\ b_0^4 b_7 + 2b_0^3 b_1 b_6 + b_0 b_1^3 b_4 + 2b_1^4 b_3 \neq 0 \\ b_8^4 b_1 + 2b_8^3 b_7 b_2 + b_8 b_7^3 b_4 + 2b_7^4 b_5 \neq 0 \end{cases} \quad (1)$$

Preuve

Soit $f = \sum a_i x^i z^{8-i} \in V_8(k)$ qui satisfait les conditions du lemme et $M = \begin{pmatrix} q & r \\ s & t \end{pmatrix} \in \mathrm{GL}_2(\overline{k})$.
On note $F = \sum A_i X^i Z^{8-i} = M.f$, pour laquelle

$$A_1 = \partial_X F(0,1) = q\partial_x f(r,t) + s\partial_y f(r,t),$$
$$A_7 = \partial_Z F(1,0) = r\partial_x f(q,s) + t\partial_y f(q,s).$$

Si $q = 0$, $A_1 = A_7 = 0$ équivaut à $2a_0 t + a_1 = 0$ et $2a_0 t^7 + a_1 t^6 + 2a_3 t^4 + a_4 t^3 + 2a_6 t + a_7 = 0$, ce qui contredit les hypothèses (résultant).

Similairement, on peut supposer $qrst \neq 0$ et seulement considérer $M = \begin{pmatrix} 1 & r \\ s & 1 \end{pmatrix}$ (modulo l'action de D).

Preuve

Pour une telle matrice M, $A_1 = A_7 = 0$ équivaut à $r = -\dfrac{\partial_z f}{\partial_x f}(1, s)$ et s est racine de

$$0 = \partial_x f(-\partial_z f(1,s), \partial_x f(1,s)) + s\partial_z f(-\partial_z f(1,s), \partial_x f(1,s)) = f(1,s)^3 P_f(s).$$

où P_f est un polynôme de degré 26.

$f(1, s) = 0$ est exlu (sinon $A8 = A7 = 0$ et $\Delta(F) = 0$).

$\mathrm{Res}_s(\partial_x f(1,s), P(s)) = (2a_1 a_8^4 + a_2 a_7 a_8^3 + 2a_4 a_7^3 a_8 + a_5 a_7^4)\,\mathrm{Disc}(f)^4 \neq 0$, ainsi toute racine $s \in K$ de P_f donne bien une solution $M_{r,s}.f \in W$.

Enfin $P_{A.f}(t) = -t^{26} P(1/t)$, où $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, ainsi les deux solutions $M_{r,s}.f$ et $M_{1/s,1/r}.f$ se confondent, soit les 13 solutions attendues.

Conclusion

- Les invariants $J_2, \ldots, J_{12}$ sont suffisants pour classifier les courbes hyperelliptiques de genre 3 définies sur un corps de caractéristique 3.
- L'espace de modules des courbes hyperelliptiques de genre 3 sur un corps de caractéristique 3 est "effectif" (stratification selon le groupe d'automorphismes, reconstruction, ...) (travail achevé).
- La caractéristique 7 peut être traitée de façon similaire (travail en cours).
- La détermination de générateurs pour $\mathcal{I}_8(\mathbb{F}_3)$ reste un problème ouvert.