Variétés abéliennes et jacobiennes de courbes hyperelliptiques, en particulier à multiplication complexe

Ivan Boyer

Sous la direction de Jean-François Mestre
Université Paris Diderot

24 janvier 2014

— Partie 1 —

Courbes à multiplication réelle

Multiplication réelle par des sous-corps de cyclotomiques

Définition (Multiplication réelle)

Une variété abélienne A est à multiplication réelle par un corps de nombres totalement réel F de dimension $\dim A$ si

$$F \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A).$$

Notation (Sous corps des cyclotomiques)

Pour $n|l-1$, on note $\mathbb{Q}(\zeta_l^{(n)})$ le sous-corps d'indice n de $\mathbb{Q}(\zeta_l)$.

Multiplication réelle par des sous-corps de cyclotomiques

Définition (Multiplication réelle)

Une variété abélienne A est à multiplication réelle par un corps de nombres totalement réel F de dimension $\dim A$ si

$$F \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A).$$

Notation (Sous corps des cyclotomiques)

Pour $n|l-1$, on note $\mathbb{Q}(\zeta_l^{(n)})$ le sous-corps d'indice n de $\mathbb{Q}(\zeta_l)$.

Multiplication réelle par des sous-corps de cyclotomiques

Théorème (Ellenberg)

n, l	*Existence théorique*
$\mathbb{Q}(\zeta_l^+)$	*famille à 3 paramètres*
$\mathbb{Q}(\zeta_l^{(4)})$	*famille à 1 paramètre*
$\mathbb{Q}(\zeta_l^{(6)})$	*famille à 1 paramètre*
$\mathbb{Q}(\zeta_l^{(8)})$	*1 courbe*
$\mathbb{Q}(\zeta_l^{(10)})$	*1 courbe*

Construction explicite

Définition (Groupes métacycliques $G_{l,n}$)

Soit l premier impair :

$$G_{l,n} = \langle \alpha, \sigma,\ \sigma^l = \alpha^n = 1, \alpha\sigma\alpha^{-1} = \sigma^k \rangle.$$

Théorème (Types de branchement, Ellenberg)

On obtient une courbe X à multiplication réelle avec les types :

n	types
2	$(0,0,1,1)$, $(0,1,1,1,1)$,$(1,1,1,1,1,1)$
4	$(0,1,1)$,$(1,1,2,2)$
6	$(1,1,2)$,$(2,2,3,3)$
8	$(1,1,4)$
10	$(1,2,5)$

Construction explicite

Définition (Groupes métacycliques $G_{l,n}$)

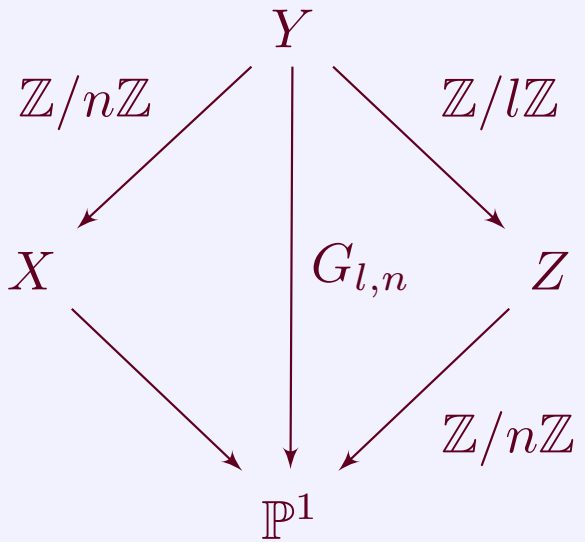
Soit l premier impair :

$$G_{l,n} = \langle \alpha, \sigma,\ \sigma^l = \alpha^n = 1, \alpha\sigma\alpha^{-1} = \sigma^k \rangle.$$

Théorème (Types de branchement, Ellenberg)

On obtient une courbe X à multiplication réelle avec les types :

n	*types*
2	$(0,0,1,1)$, $(0,1,1,1,1)$,$(1,1,1,1,1,1)$
4	$(0,1,1)$,$(1,1,2,2)$
6	$(1,1,2)$,$(2,2,3,3)$
8	$(1,1,4)$
10	$(1,2,5)$



Construction explicite

Théorème

n, l	*Existence théorique*	*Courbes explicites*	*Corps de définition*
$\mathbb{Q}(\zeta_l^+)$	*famille à 3 paramètres*	*famille à 1 paramètre* [Top] *famille à 2 paramètres* *famille à 3 paramètres*	$\mathbb{Q}$ $\mathbb{Q}$ *ext.*
$\mathbb{Q}(\zeta_l^{(4)})$	*famille à 1 paramètre*	*1 courbe* *famille à 1 paramètre*	$\mathbb{Q}(i)$ *ext.*
$\mathbb{Q}(\zeta_l^{(6)})$	*famille à 1 paramètre*	*famille à 1 paramètre* *1 courbe*	*ext.* *ext.*
$\mathbb{Q}(\zeta_l^{(8)})$	*1 courbe*	*1 courbe*	*ext.*
$\mathbb{Q}(\zeta_l^{(10)})$	*1 courbe*	*1 courbe*	*ext.*

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$ $(n=2)$

Type (0,0,1,1)

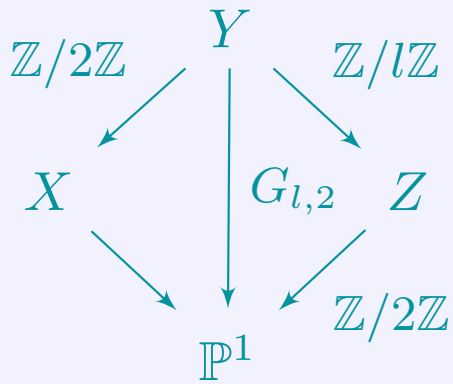
Z revêtement de $\mathbb{P}^1$ de degré 2, ramifié en 2 points : $g(Z)=0$.

Proposition (Famille à un paramètre)

La courbe Y d'équation

$$t^l = \frac{x^2+x+a}{x^2-x+a}.$$

a un revêtement $Y \to \mathbb{P}^1$, $(x,t) \mapsto x^2$ de degré $2l$, de type $(0,0,1,1)$ et de groupe de Galois le groupe diédral $G_{l,2}$.



Le quotient X fournit les courbes de [Top].

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$ $(n=2)$

Type (0,1,1,1,1)

Z est un revêtement de degré 2 ramifié en 4 points : $g(Z)=1$.

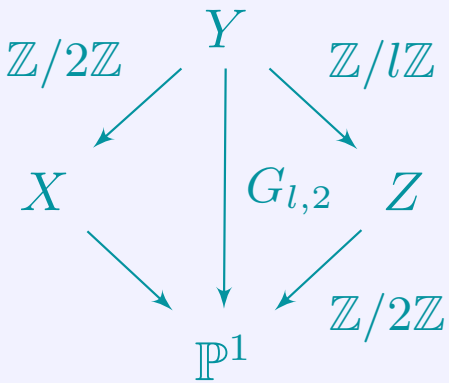
Proposition (Famille à deux paramètres)

Z courbe elliptique, $P \in Z$ et φ telle que

$$\mathrm{div}(\varphi) = (-lP) + l(P) - (l+1)O_Z.$$

Alors, Y d'équation

$$Z(x,y)=0 \text{ et } t^l = \frac{\varphi(x,y)}{\varphi(x,-y)}$$



a un revêtement $Y \to \mathbb{P}^1$, $(x,y,t) \mapsto x$ de degré $2l$, de type $(0,1,1,1,1)$ et de groupe de Galois le groupe diédral $G_{l,2}$.

Le quotient X appartient à une famille à 2 paramètres.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$ $(n=2)$

Type (0,1,1,1,1)

Proposition $(n=7)$

La famille à 2 paramètres r,t de courbes de genre3, d'éq. quartiques

$$-(2tr-r-t^3)(-r^3-40t^2r^3+10tr^3-80r^3t^4+80t^3r^3+32r^3t^5+16r^2t^7-56r^2t^6+64r^2t^5-30r^2t^4+5r^2t^3+12rt^8-16rt^7+5rt^6+t^9)+2r(2t-1)^2(r^2-4tr^2+4t^3r+4r^2t^2-10rt^4+2t^6+4rt^5)U+r^2(2t-1)^4U^2-r(2t-1)^2U^3+r(2t-1)^2(-2r^3-6r^2t^2+12tr^3+24r^2t^3-24t^2r^3-12rt^5-24r^2t^4+16t^3r^3+28rt^6-5t^8-8rt^7)V-2t^2(t^3+2r-6tr+4t^2r)^2UV-t(t^3+2r-6tr+4t^2r)(r^2-4tr^2+4t^3r+4r^2t^2-10rt^4+2t^6+4rt^5)V^2-2rt(2t-1)^2(t^3+2r-6tr+4t^2r)UV^2+t(t^3+2r-6tr+4t^2r)U^2V^2+2r(2t-1)^2(r^2-4tr^2+4t^3r+4r^2t^2-10rt^4+2t^6+4rt^5)V^3+(r^2-4tr^2+4t^3r+4r^2t^2-10rt^4+2t^6+4rt^5)UV^3+t^2(t^3+2r-6tr+4t^2r)^2V^4=0.$$

est à multiplication réelle par $\mathbb{Q}(\zeta_7^+)$.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$ $(n=2)$

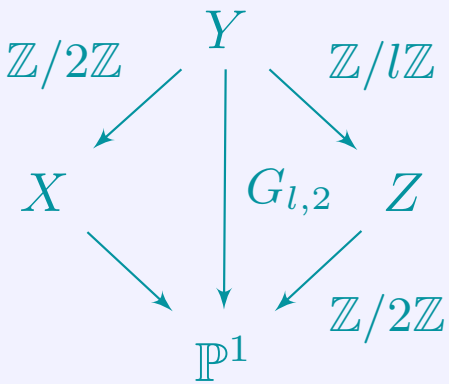
Type (1,1,1,1,1,1)

Ici Z est de genre 2 : c'est une courbe hyperelliptique. Le revêtement de Z est non ramifié.

Proposition (Famille à trois paramètres)

Soit $P \in \mathrm{Jac}(H)$ de $l-$torsion : le diviseur lP, en représentation de Mumford, est principal et s'écrit $\mathrm{div}(\varphi)$. Alors, Y d'équation

$$Z(x,y)=0 \text{ et } t^l = \frac{\varphi(x,y)}{\varphi(x,-y)}$$



a un revêtement $Y \to \mathbb{P}^1$, $(x,y,t) \mapsto x$ de degré $2l$, de type $(1,1,1,1,1,1)$ et de groupe de Galois le groupe diédral $G_{l,2}$.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$ $(n=2)$

Type (1,1,1,1,1,1)

- Nombreux exemples de familles de courbes de genre 2 avec des points rationnels de torsion.
- Par ex. : courbes modulaires hyperelliptiques de genre 2.
- De façon analogue, on peut paramétrer des courbes hyperelliptiques de genre 2, avec $P_{\infty,1} - P_{\infty,2}$ d'ordre fini.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$ $(n=2)$

Type (1,1,1,1,1,1)

- Nombreux exemples de familles de courbes de genre 2 avec des points rationnels de torsion.
- Par ex. : courbes modulaires hyperelliptiques de genre 2.
- De façon analogue, on peut paramétrer des courbes hyperelliptiques de genre 2, avec $P_{\infty,1} - P_{\infty,2}$ d'ordre fini.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$ $(n=2)$

Type (1,1,1,1,1,1)

- Nombreux exemples de familles de courbes de genre 2 avec des points rationnels de torsion.
- Par ex. : courbes modulaires hyperelliptiques de genre 2.
- De façon analogue, on peut paramétrer des courbes hyperelliptiques de genre 2, avec $P_{\infty,1} - P_{\infty,2}$ d'ordre fini.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$ $(n=2)$

Type (1,1,1,1,1,1)

- Nombreux exemples de familles de courbes de genre 2 avec des points rationnels de torsion.
- Par ex. : courbes modulaires hyperelliptiques de genre 2.
- De façon analogue, on peut paramétrer des courbes hyperelliptiques de genre 2, avec $P_{\infty,1} - P_{\infty,2}$ d'ordre fini.

Proposition ($n=5$)

Les courbes hyperelliptiques de genre 2, de la famille à deux paramètres s et t, d'équation

$$y^2 = s(16t-27+4s)x^6 + 2s(-16t+27+s)x^5 + 10stx^3 + 2t^2x + t^2,$$

sont à multiplication réelle par $\mathbb{Q}(\zeta_5^+)$.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^+)$ $(n=2)$

Type (1,1,1,1,1,1)

- Nombreux exemples de familles de courbes de genre 2 avec des points rationnels de torsion.
- Par ex. : courbes modulaires hyperelliptiques de genre 2.
- De façon analogue, on peut paramétrer des courbes hyperelliptiques de genre 2, avec $P_{\infty,1} - P_{\infty,2}$ d'ordre fini.

Proposition ($n=7$)

Voici 2 familles de courbes de genre 3*, d'équations quartiques, à multiplication réelle par* $\mathbb{Q}(\zeta_7^+)$ *(paramètres* s *et* t*)*

$$2v+u^3+(u+1)^2+s\big((u^2+v)^2-v(u+v)(2u^2-uv+2v)\big)=0$$

$$-(s+t)^2+2(s+t)sv+(-s^2+3t^2-t)v^2+(6t^2-2t-2s^2)v^3+2(s+t)^2u+(6t^2-2t-2s^2)uv^2+(-s^2+3t^2-t)uv^3-(s+t)(s-t)u^2+(2t+2s^2-6t^2)u^2v+(t-3t^2+s^2)u^2v^2+(s+t)(s-t)u^3+(2t+2s^2-6t^2)u^3v+(3t^2-t-s^2)u^4=0.$$

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^4)$ $(n=4)$

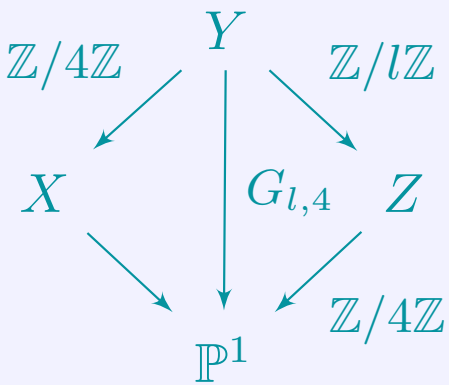
Type (0,1,1)

$Z \to \mathbb{P}^1$ de degré 4, ramifié en 2 points de degré 4 : $g(Z)=0$.

Proposition (Une courbe sur $\mathbb{Q}(i)$)

Soit $\psi(y)=\frac{(y-1)(y-i)}{(y+1)(y+i)}$ *et* $a \in \mathbb{Z}$, *d'ordre* 4 *dans* $(\mathbb{Z}/l\mathbb{Z})^*$. *On définit la courbe*

$$(Y)\begin{cases} y^4 = x \\ t^l = \psi(y)\psi(iy)^a. \end{cases}$$



Alors, le revêtement $Y \to \mathbb{P}^1$ *donné par l'application* $(x,y,t) \mapsto x$ *est de type* $(0,1,1)$.

Pour $l=13$, on trouve une équation quartique de X :

$$u^3+2u^2v+2u^2-uv^3-2uv^2-2uv-2u+v^4+v^2-v+2=0.$$

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^4)$ $(n=4)$

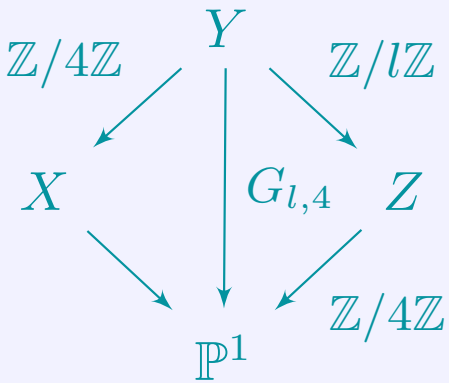
Type (0,1,1)

$Z \to \mathbb{P}^1$ de degré 4, ramifié en 2 points de degré 4 : $g(Z)=0$.

Proposition (Une courbe sur $\mathbb{Q}(i)$)

Soit $\psi(y)=\frac{(y-1)(y-i)}{(y+1)(y+i)}$ *et* $a \in \mathbb{Z}$, *d'ordre* 4 *dans* $(\mathbb{Z}/l\mathbb{Z})^*$. *On définit la courbe*

$$(Y)\begin{cases} y^4 = x \\ t^l = \psi(y)\psi(iy)^a. \end{cases}$$



Alors, le revêtement $Y \to \mathbb{P}^1$ *donné par l'application* $(x,y,t) \mapsto x$ *est de type* $(0,1,1)$.

Pour $l=13$, on trouve une équation quartique de X :

$$u^3+2u^2v+2u^2-uv^3-2uv^2-2uv-2u+v^4+v^2-v+2=0.$$

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^4)$ $(n=4)$

Type (1,1,2,2)

On a $g(Z)=1$ ou 2 et $Y \to Z$ non ramifié : $g(Z)=2$.

Proposition (Famille à un paramètre)

Soit $\tau \in \mathbb{Q}$ un paramètre $(|\tau| \neq 2)$ et soit Z la courbe hyperelliptique de genre 2, d'équation $y^2 = x(x^4+\tau x^2+1)$. Alors, l'application $(x,y) \mapsto x^2$ est un revêtement de $\mathbb{P}^1$, de degré 4 et de type $(1,1,2,2)$.

La suite se traite comme le type (1,1,1,1,1,1) avec un point d'ordre l dans la jacobienne.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^4)$ $(n=4)$

Type (1,1,2,2)

On a $g(Z)=1$ ou 2 et $Y \to Z$ non ramifié : $g(Z)=2$.

Proposition (Famille à un paramètre)

Soit $\tau \in \mathbb{Q}$ un paramètre $(|\tau| \neq 2)$ et soit Z la courbe hyperelliptique de genre 2, d'équation $y^2 = x(x^4+\tau x^2+1)$. Alors, l'application $(x,y) \mapsto x^2$ est un revêtement de $\mathbb{P}^1$, de degré 4 et de type $(1,1,2,2)$.

La suite se traite comme le type (1,1,1,1,1,1) avec un point d'ordre l dans la jacobienne.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^6)$ $(n = 6)$

Type (2,2,3,3)

- Même technique que précédemment en prenant Z d'équation $y^2 = x^6 + \tau x^3 + 1$, avec $(x, y) \mapsto x^3$ et $\alpha : (x, y) \mapsto (jx, -y)$.
- Autre technique consistant à trouver $P \in \mathrm{Jac}(Z)$ tel que $\langle P \rangle$ soit stable par α.
- « Échange » de la jacobienne algébrique à la jacobienne analytique, où il est facile de trouver un point de torsion stable.
- Grâce à ce point, extension de « Kummer » simplifiée et facilement calculable.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^6)$ $(n = 6)$

Type (2,2,3,3)

- Même technique que précédemment en prenant Z d'équation $y^2 = x^6 + \tau x^3 + 1$, avec $(x, y) \mapsto x^3$ et $\alpha : (x, y) \mapsto (jx, -y)$.
- Autre technique consistant à trouver $P \in \mathrm{Jac}(Z)$ tel que $\langle P \rangle$ soit stable par α.
- « Échange » de la jacobienne algébrique à la jacobienne analytique, où il est facile de trouver un point de torsion stable.
- Grâce à ce point, extension de « Kummer » simplifiée et facilement calculable.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^6)$ $(n = 6)$

Type (2,2,3,3)

- Même technique que précédemment en prenant Z d'équation $y^2 = x^6 + \tau x^3 + 1$, avec $(x, y) \mapsto x^3$ et $\alpha : (x, y) \mapsto (jx, -y)$.
- Autre technique consistant à trouver $P \in \mathrm{Jac}(Z)$ tel que $\langle P \rangle$ soit stable par α.
- « Échange » de la jacobienne algébrique à la jacobienne analytique, où il est facile de trouver un point de torsion stable.
- Grâce à ce point, extension de « Kummer » simplifiée et facilement calculable.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^6)$ $(n = 6)$

Type (2,2,3,3)

- Même technique que précédemment en prenant Z d'équation $y^2 = x^6 + \tau x^3 + 1$, avec $(x, y) \mapsto x^3$ et $\alpha : (x, y) \mapsto (jx, -y)$.
- Autre technique consistant à trouver $P \in \mathrm{Jac}(Z)$ tel que $\langle P \rangle$ soit stable par α.
- « Échange » de la jacobienne algébrique à la jacobienne analytique, où il est facile de trouver un point de torsion stable.
- Grâce à ce point, extension de « Kummer » simplifiée et facilement calculable.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^6)$ $(n=6)$

Type (2,2,3,3)

Proposition ($\tau = 0$, $l = 13$)

Pour x_0 racine de $x^6 + (12j+8)x^3 + \frac{1}{13}(48j+64)$ et y_0 tel que $y_0^2 = x_0^3 + 1$, le point (x_0, y_0) de la courbe elliptique $y^2 = x^3 + 1$ est d'ordre 13, et le sous-groupe qu'il engendre contient (jx_0, y_0).

Proposition

La courbe hyperelliptique suivante est à mult. réelle par $\mathbb{Q}(\sqrt{13})$.

$$Y^2 = \Big(X + (\tfrac{-(110j+115)}{468}x_0^5 + \tfrac{(289-451j)}{234}x_0^2)y_0\alpha + (\tfrac{67j+47}{156}x_0^5 + \tfrac{73j-85}{39}x_0^2)y_0\Big)\Big(X + (\tfrac{653j+337}{936}x_0^5 + \tfrac{314j-1331}{234}x_0^2)y_0\alpha + (\tfrac{47j+19}{24}x_0^5 + \tfrac{5j-110}{6}x_0^2)y_0\Big)\Big(X^2 + ((\tfrac{-(128j+57}{312})x_0^5 + \tfrac{300-29j}{78}x_0^2)y_0\alpha + (\tfrac{-(58j+11)}{72}x_0^5 + \tfrac{35j+166}{18}x_0^2)y_0)X + (\tfrac{22j+23}{13}x_0^4 + (10j-1)x_0)\alpha + \tfrac{283j+196}{52}x_0^4 + \tfrac{124j-245}{13}x_0\Big)\Big(X^2 + ((\tfrac{227j+76}{936}x_0^5 - \tfrac{11j+265}{117}x_0^2)y_0\alpha + (\tfrac{11j-8}{72}x_0{}^5 - \tfrac{20j+28}{9}x_0^2)y_0)X + (\tfrac{j-22}{52}x0^4 - \tfrac{53j+4}{13}x_0)\alpha - \tfrac{21j+45}{26}x_0^4 - \tfrac{201j+24}{13}x_0\Big)$$

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^6)$ $(n=6)$

Type (2,2,3,3)

Proposition ($\tau = 0$, $l = 13$)

Pour x_0 racine de $x^6 + (12j+8)x^3 + \frac{1}{13}(48j+64)$ et y_0 tel que $y_0^2 = x_0^3 + 1$, le point (x_0, y_0) de la courbe elliptique $y^2 = x^3 + 1$ est d'ordre 13, et le sous-groupe qu'il engendre contient (jx_0, y_0).

Proposition

La courbe hyperelliptique suivante est à mult. réelle par $\mathbb{Q}(\sqrt{13})$.

$$Y^2 = \left(X + \left(\frac{-(110j+115)}{468}x_0^5 + \frac{(289-451j)}{234}x_0^2\right)y_0\alpha + \left(\frac{67j+47}{156}x_0^5 + \frac{73j-85}{39}x_0^2\right)y_0\right)\left(X + \left(\frac{653j+337}{936}x_0^5 + \frac{314j-1331}{234}x_0^2\right)y_0\alpha + \left(\frac{47j+19}{24}x_0^5 + \frac{5j-110}{6}x_0^2\right)y_0\right)\left(X^2 + \left(\left(\frac{-(128j+57)}{312}\right)x_0^5 + \frac{300-29j}{78}x_0^2\right)y_0\alpha + \left(\frac{-(58j+11)}{72}x_0^5 + \frac{35j+166}{18}x_0^2\right)y_0\right)X + \left(\frac{22j+23}{13}x_0^4 + (10j-1)x_0\right)\alpha + \frac{283j+196}{52}x_0^4 + \frac{124j-245}{13}x_0\right)\left(X^2 + \left(\left(\frac{227j+76}{936}x_0^5 - \frac{11j+265}{117}x_0^2\right)y_0\alpha + \left(\frac{11j-8}{72}{x_0}^5 - \frac{20j+28}{9}x_0^2\right)y_0\right)X + \left(\frac{j-22}{52}{x0}^4 - \frac{53j+4}{13}x_0\right)\alpha - \frac{21j+45}{26}x_0^4 - \frac{201j+24}{13}x_0\right)$$

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^6)$, $\mathbb{Q}(\zeta_l^8)$, $\mathbb{Q}(\zeta_l^{10})$

Type (1,1,2), (1,1,4) et (1,2,5)

- À chaque fois, la méthode donne une courbe.
- Deux techniques disponibles.
- Celle par les sous-groupes stables permet de donner des équations beaucoup plus rapidement.
- Pour le type (1,2,5), Z est d'équation $y^2 = x^5 + 1$ et on ne peut pas se ramener à une courbe elliptique : on utilise la théorie de la multiplication complexe.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^6)$, $\mathbb{Q}(\zeta_l^8)$, $\mathbb{Q}(\zeta_l^{10})$

Type (1,1,2), (1,1,4) et (1,2,5)

- À chaque fois, la méthode donne une courbe.
- Deux techniques disponibles.
- Celle par les sous-groupes stables permet de donner des équations beaucoup plus rapidement.
- Pour le type (1,2,5), Z est d'équation $y^2 = x^5 + 1$ et on ne peut pas se ramener à une courbe elliptique : on utilise la théorie de la multiplication complexe.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^6)$, $\mathbb{Q}(\zeta_l^8)$, $\mathbb{Q}(\zeta_l^{10})$

Type (1,1,2), (1,1,4) et (1,2,5)

- À chaque fois, la méthode donne une courbe.
- Deux techniques disponibles.
- Celle par les sous-groupes stables permet de donner des équations beaucoup plus rapidement.
- Pour le type (1,2,5), Z est d'équation $y^2 = x^5 + 1$ et on ne peut pas se ramener à une courbe elliptique : on utilise la théorie de la multiplication complexe.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^6)$, $\mathbb{Q}(\zeta_l^8)$, $\mathbb{Q}(\zeta_l^{10})$

Type (1,1,2), (1,1,4) et (1,2,5)

- À chaque fois, la méthode donne une courbe.
- Deux techniques disponibles.
- Celle par les sous-groupes stables permet de donner des équations beaucoup plus rapidement.
- Pour le type (1,2,5), Z est d'équation $y^2 = x^5 + 1$ et on ne peut pas se ramener à une courbe elliptique : on utilise la théorie de la multiplication complexe.

Courbes à multiplication réelle par $\mathbb{Q}(\zeta_l^6)$, $\mathbb{Q}(\zeta_l^8)$, $\mathbb{Q}(\zeta_l^{10})$

Type (1,1,2), (1,1,4) et (1,2,5)

Proposition

Les points suivants engendrent des groupes d'ordre l, stables par $(x,y) \mapsto (\zeta_5 x, y)$.

1. $l = 11$. *γ racine de* $t^5 + \frac{1}{121}(80\zeta_5^3 + 320\zeta_5^2 + 1040\zeta_5 + 1264)$ *et δ une racine de* $t^2 + \frac{1}{11}(-36\zeta_5^3 - 12\zeta_5^2 - 28\zeta_5 + 1)$. *Alors*

   $$P = \left(t^2 + \tfrac{1}{4}(\zeta_5^3 + 2\zeta_5)\gamma^3 t + \gamma, \tfrac{1}{22}(-\zeta_5^3 + \zeta_5^2 + 8\zeta_5 - 6)\gamma^2\delta t + \delta\right)$$

   est d'ordre 11 *et vérifie* $\alpha(P) = 2P$.
2. $l = 31$. *On donne des équations pour un point P de la jacobienne de* $y^2 = x^5 + 1$ *tel que* $31P = 0$ *et* $\alpha(P) = -2P$.

— Partie 2 —

Factorisation dans $\mathbb{F}_p[t]$ et multiplication complexe

La situation

- Pas d'algorithmes déterministes polynomiaux pour factoriser les polynômes dans $\mathbb{F}_p[X]$.
- Même en degré 2 : Schoof donne un algorithme pour calculer une racine carrée de la réduction d'un entier fixé dans $\mathbb{F}_p$.
- Avec les courbes de Fermat $x^l+y^l=z^l$, Pila étend le résultat aux racines l-ième de l'unité, sous certaines conditions.
- On propose ici de généraliser ce résultat aux extensions abéliennes, en utilisant d'autres courbes.

La situation

- Pas d'algorithmes déterministes polynomiaux pour factoriser les polynômes dans $\mathbb{F}_p[X]$.
- Même en degré 2 : Schoof donne un algorithme pour calculer une racine carrée de la réduction d'un entier fixé dans $\mathbb{F}_p$.
- Avec les courbes de Fermat $x^l+y^l=z^l$, Pila étend le résultat aux racines l-ième de l'unité, sous certaines conditions.
- On propose ici de généraliser ce résultat aux extensions abéliennes, en utilisant d'autres courbes.

La situation

- Pas d'algorithmes déterministes polynomiaux pour factoriser les polynômes dans $\mathbb{F}_p[X]$.
- Même en degré 2 : Schoof donne un algorithme pour calculer une racine carrée de la réduction d'un entier fixé dans $\mathbb{F}_p$.
- Avec les courbes de Fermat $x^l+y^l=z^l$, Pila étend le résultat aux racines l-ième de l'unité, sous certaines conditions.
- On propose ici de généraliser ce résultat aux extensions abéliennes, en utilisant d'autres courbes.

La situation

- Pas d'algorithmes déterministes polynomiaux pour factoriser les polynômes dans $\mathbb{F}_p[X]$.
- Même en degré 2 : Schoof donne un algorithme pour calculer une racine carrée de la réduction d'un entier fixé dans $\mathbb{F}_p$.
- Avec les courbes de Fermat $x^l+y^l=z^l$, Pila étend le résultat aux racines l-ième de l'unité, sous certaines conditions.
- On propose ici de généraliser ce résultat aux extensions abéliennes, en utilisant d'autres courbes.

Utilisation de la multiplication complexe

- On considère une variété abélienne à multiplication complexe par $\mathbb{Q}(\zeta_l)$.
- On sait – algorithme de Pila – calculer le nombre de points et donc la fonction ζ en temps polynomial, déterministe.
- Cela fournit le polynôme caractéristique du Frobenius.
- Par la théorie de la multiplication complexe, on sait que

$$(\pi^f) = \prod_{i=1}^{n} \varphi_i^{-1}(\mathfrak{P}) = \prod_{i=1}^{g} \psi_i(\mathfrak{P})^{h_i},$$

où $\varphi_1, \ldots, \varphi_n$ est le type-CM, $\{\psi_1, \ldots, \psi_g\} = \mathrm{Gal}(K_0/\mathbb{Q})$ et f est l'ordre de p dans $(\mathbb{Z}/l\mathbb{Z})^*$

Utilisation de la multiplication complexe

- On considère une variété abélienne à multiplication complexe par $\mathbb{Q}(\zeta_l)$.
- On sait – algorithme de Pila – calculer le nombre de points et donc la fonction ζ en temps polynomial, déterministe.
- Cela fournit le polynôme caractéristique du Frobenius.
- Par la théorie de la multiplication complexe, on sait que

$$(\pi^f) = \prod_{i=1}^{n} \varphi_i^{-1}(\mathfrak{P}) = \prod_{i=1}^{g} \psi_i(\mathfrak{P})^{h_i},$$

où $\varphi_1, \ldots, \varphi_n$ est le type-CM, $\{\psi_1, \ldots, \psi_g\} = \mathrm{Gal}(K_0/\mathbb{Q})$ et f est l'ordre de p dans $(\mathbb{Z}/l\mathbb{Z})^*$

Utilisation de la multiplication complexe

- On considère une variété abélienne à multiplication complexe par $\mathbb{Q}(\zeta_l)$.
- On sait – algorithme de Pila – calculer le nombre de points et donc la fonction ζ en temps polynomial, déterministe.
- Cela fournit le polynôme caractéristique du Frobenius.
- Par la théorie de la multiplication complexe, on sait que

$$(\pi^f) = \prod_{i=1}^{n} \varphi_i^{-1}(\mathfrak{P}) = \prod_{i=1}^{g} \psi_i(\mathfrak{P})^{h_i},$$

où $\varphi_1, \ldots, \varphi_n$ est le type-CM, $\{\psi_1, \ldots, \psi_g\} = \mathrm{Gal}(K_0/\mathbb{Q})$ et f est l'ordre de p dans $(\mathbb{Z}/l\mathbb{Z})^*$

Utilisation de la multiplication complexe

- On considère une variété abélienne à multiplication complexe par $\mathbb{Q}(\zeta_l)$.
- On sait – algorithme de Pila – calculer le nombre de points et donc la fonction ζ en temps polynomial, déterministe.
- Cela fournit le polynôme caractéristique du Frobenius.
- Par la théorie de la multiplication complexe, on sait que

$$\left(\pi^f\right) = \prod_{i=1}^{n} \varphi_i^{-1}(\mathfrak{P}) = \prod_{i=1}^{g} \psi_i(\mathfrak{P})^{h_i},$$

où $\varphi_1, \ldots, \varphi_n$ est le type-CM, $\{\psi_1, \ldots, \psi_g\} = \mathrm{Gal}(K_0/\mathbb{Q})$ et f est l'ordre de p dans $(\mathbb{Z}/l\mathbb{Z})^*$

Propriété de séparation

Définition (Séparation)

On dira que les idéaux $\mathfrak{P}_i$ et $\mathfrak{P}_j$, pour $i \neq j$, sont séparés s'il existe $\psi \in \mathrm{Gal}(K_0/\mathbb{Q})$ tel que

$$\nu_\psi(i) \neq \nu_\psi(j).$$

Si tous les idéaux sont séparés, on dit que l'on a la propriété de séparation.

Théorème

On a la propriété de séparation si et seulement si $\mathbb{Q}(\pi^f)$ est le corps K_0 de décomposition de (p) dans $\mathbb{Q}(\zeta_l)$.

Propriété de séparation

Définition (Séparation)

On dira que les idéaux $\mathfrak{P}_i$ et $\mathfrak{P}_j$, pour $i \neq j$, sont séparés s'il existe $\psi \in \mathrm{Gal}(K_0/\mathbb{Q})$ tel que

$$\nu_\psi(i) \neq \nu_\psi(j).$$

Si tous les idéaux sont séparés, on dit que l'on a la propriété de séparation.

Théorème

On a la propriété de séparation si et seulement si $\mathbb{Q}(\pi^f)$ est le corps K_0 de décomposition de (p) dans $\mathbb{Q}(\zeta_l)$.

Propriété de séparation

Corollaire

Si (p) est totalement décomposé dans $\mathbb{Q}(\zeta_l)$ alors, on a la propriété de séparation si et seulement si le type-CM est primitif.

Exemple

Si $p \equiv 1[l]$ alors, pour $A = \mathrm{Jac}(y^2 = x^l - 1)$, on a la propriété de séparation.

Propriété de séparation

Corollaire

Si (p) est totalement décomposé dans $\mathbb{Q}(\zeta_l)$ alors, on a la propriété de séparation si et seulement si le type-CM est primitif.

Exemple

Si $p \equiv 1[l]$ alors, pour $A = \mathrm{Jac}(y^2 = x^l - 1)$, on a la propriété de séparation.

Propriété de séparation et factorisation

Théorème

Soit l un entier premier impair fixé. Soit A une variété abélienne à multiplication complexe par $\mathbb{Q}(\zeta_l)$ et soit f l'ordre de p dans $(\mathbb{Z}/l\mathbb{Z})^*$ et π le Frobenius de A modulo p.
On suppose que $\mathbb{Q}(\pi^f)$ coïncide avec le corps de décomposition de (p) dans $\mathbb{Q}(\zeta_l)$. Alors, il existe un algorithme déterministe en temps polynomial en $\log(p)$ qui donne la factorisation de $\Phi_l \in \mathbb{F}_p[t]$.

Corollaire (Résultat de Pila)

Si $p \equiv 1[l]$, il existe un algorithme polynomial déterministe qui donne les racines l-ième de l'unité en temps polynomial déterministe.

Propriété de séparation et factorisation

Théorème

Soit l un entier premier impair fixé. Soit A une variété abélienne à multiplication complexe par $\mathbb{Q}(\zeta_l)$ et soit f l'ordre de p dans $(\mathbb{Z}/l\mathbb{Z})^*$ et π le Frobenius de A modulo p.
On suppose que $\mathbb{Q}(\pi^f)$ coïncide avec le corps de décomposition de (p) dans $\mathbb{Q}(\zeta_l)$. Alors, il existe un algorithme déterministe en temps polynomial en $\log(p)$ qui donne la factorisation de $\Phi_l \in \mathbb{F}_p[t]$.

Corollaire (Résultat de Pila)

Si $p \equiv 1[l]$, il existe un algorithme polynomial déterministe qui donne les racines l-ième de l'unité en temps polynomial déterministe.

Généralisations : p d'ordre impair

- On utilise encore $\mathrm{Jac}(y^2 = x^l - 1)$.

Corollaire

l premier impair fixé et p premier, d'ordre f impair dans $(\mathbb{Z}/l\mathbb{Z})^*$. On a un algorithme factorisant $\Phi_l(t) \in \mathbb{F}_p[t]$ en temps polynomial.

- On utilise cette fois $\mathrm{Jac}(y^2 = x^{l^m} - 1)$.

Corollaire

Soit p premier impair d'ordre impair dans $(\mathbb{Z}/l\mathbb{Z})^*$. On a un algorithme factorisant $\Phi_{l^m}(t) \in \mathbb{F}_p[t]$ en temps polynomial.

Corollaire

Il existe un algorithme polynomial en $\log(p)$ qui donne la factorisation de $\Phi_{2^m}(t) \in \mathbb{F}_p[t]$ pour $m > 1$ et $p = 1 \mod 2^m$.

Généralisations : p d'ordre impair

- On utilise encore $\mathrm{Jac}(y^2 = x^l - 1)$.

Corollaire

l premier impair fixé et p premier, d'ordre f impair dans $(\mathbb{Z}/l\mathbb{Z})^*$. On a un algorithme factorisant $\Phi_l(t) \in \mathbb{F}_p[t]$ en temps polynomial.

- On utilise cette fois $\mathrm{Jac}(y^2 = x^{l^m} - 1)$.

Corollaire

Soit p premier impair d'ordre impair dans $(\mathbb{Z}/l\mathbb{Z})^*$. On a un algorithme factorisant $\Phi_{l^m}(t) \in \mathbb{F}_p[t]$ en temps polynomial.

Corollaire

Il existe un algorithme polynomial en $\log(p)$ qui donne la factorisation de $\Phi_{2^m}(t) \in \mathbb{F}_p[t]$ pour $m > 1$ et $p = 1 \mod 2^m$.

Généralisations : p d'ordre impair

Algorithme (Factorisation de $\Phi_l(t) \in \mathbb{F}_p[t]$)

Entrée : *(p, l) avec p d'ordre f impair dans $(\mathbb{Z}/l\mathbb{Z})^*$; $g = \frac{l-1}{f}$.*

1: $\Pi(t^f) \leftarrow$ *Fonction-Zêta*$(y^2 = x^l - 1)$
2: *Factoriser $\Pi(t)$ dans $\mathbb{Q}(\zeta_l)[t]$ grâce à* LLL *par exemple*
3: *Soient $P_1, \ldots, P_g$ tels que $\Pi(t) = \prod_{j=1}^{g} \left(t - P_j(\zeta_l)\right)$ (factorisation ci-dessus)*
4: $Q_j \leftarrow \mathrm{pgcd}_{\mathbb{F}_p}\left(\frac{P_j}{p^k}, \Phi_l\right)$ *avec k maximal*
5: $F \leftarrow Q_1$, $j \leftarrow 2$
6: ***Répéter***
7: $\quad F' \leftarrow$ *pgcd*$(F, Q_j) \mod p$
8: $\quad$ ***Si*** $F' \neq 1$ ***Alors***
9: $\quad\quad F \leftarrow F'$
10: $\quad$ ***Fin Si***
11: $\quad j \leftarrow j + 1$
12: ***Jusqu'à*** $\deg F = f$
13: ***Recommencer*** *en 5 avec les numérateurs de $Q_1/F, \ldots, Q_g/F$ modulo p.*
14: ***Jusqu'à*** *ce que les g facteurs de Φ_l soient déterminés.*

Généralisations : p d'ordre impair

- On utilise encore $\mathrm{Jac}(y^2 = x^l - 1)$.

Corollaire

l premier impair fixé et p premier, d'ordre f impair dans $(\mathbb{Z}/l\mathbb{Z})^*$. On a un algorithme factorisant $\Phi_l(t) \in \mathbb{F}_p[t]$ en temps polynomial.

- On utilise cette fois $\mathrm{Jac}(y^2 = x^{l^m} - 1)$.

Corollaire

Soit p premier impair d'ordre impair dans $(\mathbb{Z}/l\mathbb{Z})^*$. On a un algorithme factorisant $\Phi_{l^m}(t) \in \mathbb{F}_p[t]$ en temps polynomial.

Corollaire

Il existe un algorithme polynomial en $\log(p)$ qui donne la factorisation de $\Phi_{2^m}(t) \in \mathbb{F}_p[t]$ pour $m > 1$ et $p \equiv 1 \mod 2^m$.

Généralisations : p d'ordre impair

- On utilise encore $\mathrm{Jac}(y^2 = x^l - 1)$.

Corollaire

l premier impair fixé et p premier, d'ordre f impair dans $(\mathbb{Z}/l\mathbb{Z})^*$. On a un algorithme factorisant $\Phi_l(t) \in \mathbb{F}_p[t]$ en temps polynomial.

- On utilise cette fois $\mathrm{Jac}(y^2 = x^{l^m} - 1)$.

Corollaire

Soit p premier impair d'ordre impair dans $(\mathbb{Z}/l\mathbb{Z})^*$. On a un algorithme factorisant $\Phi_{l^m}(t) \in \mathbb{F}_p[t]$ en temps polynomial.

Corollaire

Il existe un algorithme polynomial en $\log(p)$ qui donne la factorisation de $\Phi_{2^m}(t) \in \mathbb{F}_p[t]$ pour $m > 1$ et $p \equiv 1 \mod 2^m$.

Généralisations : p d'ordre impair

- On utilise encore $\mathrm{Jac}(y^2 = x^l - 1)$.

Corollaire

l premier impair fixé et p premier, d'ordre f impair dans $(\mathbb{Z}/l\mathbb{Z})^*$. On a un algorithme factorisant $\Phi_l(t) \in \mathbb{F}_p[t]$ en temps polynomial.

- On utilise cette fois $\mathrm{Jac}(y^2 = x^{l^m} - 1)$.

Corollaire

Soit p premier impair d'ordre impair dans $(\mathbb{Z}/l\mathbb{Z})^*$. On a un algorithme factorisant $\Phi_{l^m}(t) \in \mathbb{F}_p[t]$ en temps polynomial.

Corollaire

Il existe un algorithme polynomial en $\log(p)$ qui donne la factorisation de $\Phi_{2^m}(t) \in \mathbb{F}_p[t]$ pour $m > 1$ et $p \equiv 1 \mod 2^m$.

Généralisations : p d'ordre pair

- Avec une courbe de la famille de [Top], vue au début, quotient de $y^2 = x^{2l+1} + x$, à multiplication complexe par $\mathbb{Q}(\zeta_l^+, i)$.

Proposition

Si p est d'ordre 2 et $p \equiv 1 \mod 4$ alors, on a encore un algorithme de factorisation.

- Avec la même courbe :

Conjecture (vérifiée pour $l \leqslant 1000$)

Le résultat est encore valable, sans l'hypothèse p d'ordre 2.

- Toutefois, avec $y^2 = x^{4l+1} + x$:

Conjecture (vérifiée pour $l \leqslant 150$)

On a un algorithme de factorisation pour $p \not\equiv 1 \mod 8$

Généralisations : p d'ordre pair

- Avec une courbe de la famille de [Top], vue au début, quotient de $y^2 = x^{2l+1} + x$, à multiplication complexe par $\mathbb{Q}(\zeta_l^+, i)$.

Proposition

Si p est d'ordre 2 et $p \equiv 1 \mod 4$ alors, on a encore un algorithme de factorisation.

- Avec la même courbe :

Conjecture (vérifiée pour $l \leqslant 1000$)

Le résultat est encore valable, sans l'hypothèse p d'ordre 2.

- Toutefois, avec $y^2 = x^{4l+1} + x$:

Conjecture (vérifiée pour $l \leqslant 150$)

On a un algorithme de factorisation pour $p \not\equiv 1 \mod 8$

Généralisations : p d'ordre pair

- Avec une courbe de la famille de [Top], vue au début, quotient de $y^2 = x^{2l+1} + x$, à multiplication complexe par $\mathbb{Q}(\zeta_l^+, i)$.

Proposition

Si p est d'ordre 2 et $p \equiv 1 \mod 4$ alors, on a encore un algorithme de factorisation.

- Avec la même courbe :

Conjecture (vérifiée pour $l \leqslant 1000$)

Le résultat est encore valable, sans l'hypothèse p d'ordre 2.

- Toutefois, avec $y^2 = x^{4l+1} + x$:

Conjecture (vérifiée pour $l \leqslant 150$)

On a un algorithme de factorisation pour $p \not\equiv 1 \mod 8$

Une autre approche

Contourner les conjectures

- Construire directement une variété abélienne avec un type-CM primitif et un corps de décomposition adéquat.
- On connaît l'existence de telles variétés abéliennes
- On peut construire les périodes sur $\mathbb{C}$ et interpoler ensuite.
- Pas de moyens généraux pour vérifier que la variété abélienne obtenue a le bon anneau d'endomorphismes.

Une autre approche

Contourner les conjectures

- Construire directement une variété abélienne avec un type-CM primitif et un corps de décomposition adéquat.
- On connaît l'existence de telles variétés abéliennes
- On peut construire les périodes sur $\mathbb{C}$ et interpoler ensuite.
- Pas de moyens généraux pour vérifier que la variété abélienne obtenue a le bon anneau d'endomorphismes.

Une autre approche

Contourner les conjectures

- Construire directement une variété abélienne avec un type-CM primitif et un corps de décomposition adéquat.
- On connaît l'existence de telles variétés abéliennes
- On peut construire les périodes sur $\mathbb{C}$ et interpoler ensuite.
- Pas de moyens généraux pour vérifier que la variété abélienne obtenue a le bon anneau d'endomorphismes.

Une autre approche

Contourner les conjectures

- Construire directement une variété abélienne avec un type-CM primitif et un corps de décomposition adéquat.
- On connaît l'existence de telles variétés abéliennes
- On peut construire les périodes sur $\mathbb{C}$ et interpoler ensuite.
- Pas de moyens généraux pour vérifier que la variété abélienne obtenue a le bon anneau d'endomorphismes.

Une autre approche : exemple pour $\mathbb{Q}(\zeta_{13}^{(4)}, i)$

Recherche d'une variété abélienne

- On construit l'anneau des endomorphismes avec le type-CM adéquat.
- On calcule les fonction thêta associées.
- C'est la jacobienne d'une courbe hyperelliptique.
- Avec la formule de Thomae, on peut en déduire un modèle de Rosenhain.
- On utilise les invariants d'Igusa, pour déterminer un corps de nombres sur lequel est définie la courbe. On trouve $\mathbb{Q}(\beta)$ le corps de nombres défini par $\beta^3 - \beta^2 + 9\beta - 1$ et la courbe hyperelliptique $\mathscr{H}$

$$y^2 = f(x) = x\left(x^6 + \frac{\beta^2 - 4\beta - 1}{2}x^4 - \frac{\beta^2 - 12\beta + 1}{2}x^2 - \beta^2\right).$$

Une autre approche : exemple pour $\mathbb{Q}(\zeta_{13}^{(4)}, i)$

Recherche d'une variété abélienne

- On construit l'anneau des endomorphismes avec le type-CM adéquat.
- On calcule les fonction thêta associées.
- C'est la jacobienne d'une courbe hyperelliptique.
- Avec la formule de Thomae, on peut en déduire un modèle de Rosenhain.
- On utilise les invariants d'Igusa, pour déterminer un corps de nombres sur lequel est définie la courbe. On trouve $\mathbb{Q}(\beta)$ le corps de nombres défini par $\beta^3 - \beta^2 + 9\beta - 1$ et la courbe hyperelliptique $\mathscr{H}$

$$y^2 = f(x) = x\left(x^6 + \frac{\beta^2 - 4\beta - 1}{2}x^4 - \frac{\beta^2 - 12\beta + 1}{2}x^2 - \beta^2\right).$$

Une autre approche : exemple pour $\mathbb{Q}(\zeta_{13}^{(4)}, i)$

Recherche d'une variété abélienne

- On construit l'anneau des endomorphismes avec le type-CM adéquat.
- On calcule les fonction thêta associées.
- C'est la jacobienne d'une courbe hyperelliptique.
- Avec la formule de Thomae, on peut en déduire un modèle de Rosenhain.
- On utilise les invariants d'Igusa, pour déterminer un corps de nombres sur lequel est définie la courbe. On trouve $\mathbb{Q}(\beta)$ le corps de nombres défini par $\beta^3 - \beta^2 + 9\beta - 1$ et la courbe hyperelliptique $\mathscr{H}$

$$y^2 = f(x) = x\left(x^6 + \frac{\beta^2 - 4\beta - 1}{2}x^4 - \frac{\beta^2 - 12\beta + 1}{2}x^2 - \beta^2\right).$$

Une autre approche : exemple pour $\mathbb{Q}(\zeta_{13}^{(4)}, i)$

Recherche d'une variété abélienne

- On construit l'anneau des endomorphismes avec le type-CM adéquat.
- On calcule les fonction thêta associées.
- C'est la jacobienne d'une courbe hyperelliptique.
- Avec la formule de Thomae, on peut en déduire un modèle de Rosenhain.
- On utilise les invariants d'Igusa, pour déterminer un corps de nombres sur lequel est définie la courbe. On trouve $\mathbb{Q}(\beta)$ le corps de nombres défini par $\beta^3 - \beta^2 + 9\beta - 1$ et la courbe hyperelliptique $\mathscr{H}$

$$y^2 = f(x) = x\left(x^6 + \frac{\beta^2 - 4\beta - 1}{2}x^4 - \frac{\beta^2 - 12\beta + 1}{2}x^2 - \beta^2\right).$$

Une autre approche : exemple pour $\mathbb{Q}(\zeta_{13}^{(4)}, i)$

Recherche d'une variété abélienne

- On construit l'anneau des endomorphismes avec le type-CM adéquat.
- On calcule les fonction thêta associées.
- C'est la jacobienne d'une courbe hyperelliptique.
- Avec la formule de Thomae, on peut en déduire un modèle de Rosenhain.
- On utilise les invariants d'Igusa, pour déterminer un corps de nombres sur lequel est définie la courbe. On trouve $\mathbb{Q}(\beta)$ le corps de nombres défini par $\beta^3 - \beta^2 + 9\beta - 1$ et la courbe hyperelliptique $\mathscr{H}$

$$y^2 = f(x) = x\left(x^6 + \frac{\beta^2 - 4\beta - 1}{2}x^4 - \frac{\beta^2 - 12\beta + 1}{2}x^2 - \beta^2\right).$$

Une autre approche : exemple pour $\mathbb{Q}(\zeta_{13}^{(4)}, i)$

Vérification de la multiplication complexe

- La multiplication par $[i]$ se lit sur l'équation de $\mathscr{H}$.
- Par les mêmes calculs approchés sur les endomorphismes :

Proposition

Il existe une correspondance $8-3$ sur $\mathscr{H} \times \mathscr{H}$.

$$\begin{cases} y^2 = f(x) \\ y'^2 = f(x') \\ 0 = C(x,x') \\ yy' = V(x,x') \mod C(x,x') \end{cases}$$

L'endomorphisme induit engendre la multiplication réelle (calcul de son action sur les différentielles), et commute à $[i]$.

Une autre approche : exemple pour $\mathbb{Q}(\zeta_{13}^{(4)}, i)$

Vérification de la multiplication complexe

- La multiplication par $[i]$ se lit sur l'équation de $\mathscr{H}$.
- Par les mêmes calculs approchés sur les endomorphismes :

Proposition

Il existe une correspondance $8-3$ sur $\mathscr{H} \times \mathscr{H}$.

$$\begin{cases} y^2 = f(x) \\ y'^2 = f(x') \\ 0 = C(x,x') \\ yy' = V(x,x') \mod C(x,x') \end{cases}$$

L'endomorphisme induit engendre la multiplication réelle (calcul de son action sur les différentielles), et commute à $[i]$.

Une autre approche : exemple pour $\mathbb{Q}(\zeta_{13}^{(4)}, i)$

Vérification de la multiplication complexe

- La multiplication par $[i]$ se lit sur l'équation de $\mathscr{H}$.
- Par les mêmes calculs approchés sur les endomorphismes :

Proposition

Il existe une correspondance $8-3$ *sur* $\mathscr{H} \times \mathscr{H}$.

$$\begin{cases} y^2 = f(x) \\ y'^2 = f(x') \\ 0 = C(x,x') \\ yy' = V(x,x') \mod C(x,x') \end{cases}$$

L'endomorphisme induit engendre la multiplication réelle (calcul de son action sur les différentielles), et commute à $[i]$.

Une autre approche : exemple pour $\mathbb{Q}(\zeta_{13}^{(4)}, i)$

Vérification de la multiplication complexe

- La multiplication par $[i]$ se lit sur l'équation de $\mathscr{H}$.
- Par les mêmes calculs approchés sur les endomorphismes :

Proposition

Il existe une correspondance $8-3$ *sur* $\mathscr{H} \times \mathscr{H}$.

$$\begin{cases} y^2 = f(x) \\ y'^2 = f(x') \\ 0 = C(x,x') \\ yy' = V(x,x') \mod C(x,x') \end{cases}$$

L'endomorphisme induit engendre la multiplication réelle (calcul de son action sur les différentielles), et commute à $[i]$.

Une autre approche : exemple pour $\mathbb{Q}(\zeta_{13}^{(4)}, i)$

Les équations !

La correspondance est définie sur le corps de classe de Hilbert défini par $\mathbb{Q}(a)$ avec

$$a^9 - a^8 - 2a^7 - a^6 + 5a^5 + a^4 - 5a^3 + 2a^2 + 2a - 1 = 0.$$

$$C = ((-10a^8 + 10a^7 + 24a^6 + 16a^5 - 54a^4 - 26a^3 + 40a^2 - 10a - 26)x^7 + (-2a^8 + 4a^7 - 6a^6 + 4a^5 - 2a^4 + 20a^3 - 18a^2 - 16a + 30)x^5 + (8a^8 - 10a^7 + 6a^6 - 24a^5 + 10a^4 - 38a^3 + 52a^2 + 50a - 36)x^3 + (14a^8 - 12a^7 - 36a^6 - 20a^5 + 82a^4 + 52a^3 - 76a^2 - 20a + 18)x)z^3 + (2x^8 + (-6a^7 + 10a^6 + 2a^5 + 4a^4 - 30a^3 + 26a^2 + 16a - 30)x^6 + (19a^8 - 16a^7 - 44a^6 - 26a^5 + 99a^4 + 53a^3 - 100a^2 + 30)x^4 + (-28a^8 + 15a^7 + 70a^6 + 63a^5 - 129a^4 - 120a^3 + 97a^2 + 36a - 27)x^2 - 21a^8 + 8a^7 + 57a^6 + 54a^5 - 95a^4 - 111a^3 + 67a^2 + 47a - 22)z^2 + ((-2a^7 - 4a^6 + 6a^5 + 14a^4 + 4a^3 - 24a^2 - 8a + 16)x^7 + (2a^8 + 11a^7 + 17a^6 - 47a^5 - 79a^4 - 12a^3 + 146a^2 + 65a - 63)x^5 + (31a^8 - 18a^7 - 144a^6 - 18a^5 + 271a^4 + 283a^3 - 388a^2 - 204a + 142)x^3 + (-43a^8 + 41a^7 + 56a^6 + 91a^5 - 164a^4 - 23a^3 + 27a^2 - 76a + 37)x)z + ((23a^8 - 20a^7 - 46a^6 - 42a^5 + 113a^4 + 53a^3 - 72a^2 - 6a + 14)x^6 + (-94a^8 + 25a^7 + 217a^6 + 291a^5 - 309a^4 - 430a^3 + 88a^2 + 97a - 19)x^4 + (-5a^8 + 145a^7 - 42a^6 - 293a^5 - 442a^4 + 461a^3 + 575a^2 - 118a - 89)x^2 + 61a^8 - 11a^7 - 191a^6 - 167a^5 + 278a^4 + 411a^3 - 236a^2 - 195a + 93)$$

Une autre approche : exemple pour $\mathbb{Q}(\zeta_{13}^{(4)}, i)$

Les équations !

$$V = \Big((x-a+1)(x+a-1)(x-2a^8+2a^7+3a^6+3a^5-9a^4-a^3+6a^2-3a)(x+2a^8-2a^7-3a^6-3a^5+9a^4+a^3-6a^2+3a)(x^{10}z^2+1/2(-a^8-3a^7+4a^6+8a^5+6a^4-14a^3-6a^2+a-1)x^9z+1/2(31a^8-18a^7-68a^6-64a^5+128a^4+86a^3-104a^2+9a+50)x^8z^2+1/2(-a^8-2a^7+8a^6-3a^4-16a^3+25a^2-2a-15)x^8+1/2(28a^8-34a^7-6a^6-61a^5+75a^4-78a^3+63a^2+134a-66)x^7z+1/2(-76a^8+46a^7+167a^6+159a^5-320a^4-225a^3+240a^2-4a-94)x^6z^2+1/4(63a^8-64a^7-57a^6-121a^5+189a^4-61a^3-17a^2+274a-83)x^6+1/4(51a^8-44a^7-224a^6+8a^5+452a^4+400a^3-694a^2-221a+190)x^5z+1/4(149a^8-48a^7-285a^6-465a^5+403a^4+489a^3-5a^2+46a+13)x^4z^2+1/4(315a^8-252a^7-1020a^6-354a^5+2188a^4+1714a^3-2452a^2-1031a+734)x^4+1/4(-137a^8+134a^7+219a^6+255a^5-615a^4-163a^3+277a^2-134a+41)x^3z+1/4(-85a^8-79a^7+198a^6+506a^5+88a^4-644a^3-462a^2+83a+89)x^2z^2+1/4(-1080a^8+467a^7+2625a^6+2825a^5-4453a^4-4843a^3+2561a^2+1445a-612)x^2+1/4(264a^8+173a^7-643a^6-1385a^5+39a^4+1909a^3+961a^2-341a-212)xz+1/4(119a^8-147a^7-325a^6-55a^5+911a^4+375a^3-961a^2-262a+258)z^2+1/4(-356a^8+500a^7+977a^6+15a^5-2953a^4-983a^3+3227a^2+795a-849)\Big)\Big/\Big(x(x-a^8+a^7+2a^6+2a^5-5a^4-2a^3+2a^2-a)(x+a^8-a^7-2a^6-2a^5+5a^4+2a^3-2a^2+a)(x^2+a^8-2a^7-a^6-a^5+6a^4-2a^3-a^2+4a-2)^3\Big)$$

Une autre approche : exemple pour $\mathbb{Q}(\zeta_{13}^{(4)}, i)$

Les équations !

L'action sur la base de différentielles holomorphes

$$\left\{ \frac{\mathrm{d}x}{y}, x\frac{\mathrm{d}x}{y}, x^2\frac{\mathrm{d}x}{y} \right\}$$

est donnée par la matrice

$$\begin{pmatrix} 2a^8-3a^6-5a^5+4a^4+3a^3-5a^2+2 & 0 & -9a^8+2a^7+16a^6+21a^5-25a^4-19a^3+26a^2-12 \\ 0 & \gamma & 0 \\ 3a^8-5a^7-2a^6-2a^5+16a^4-9a^3-7a^2+9a-2 & 0 & -3a^8+a^7+6a^6+7a^5-10a^4-8a^3+9a^2+a-5 \end{pmatrix}$$

où $\gamma = a^8-a^7-3a^6-2a^5+6a^4+5a^3-4a^2-a+2 \in \mathbb{Q}\left(\zeta_{13}^{(4)}\right)$.

Son polynôme minimal est $X^3 + X^2 - 4X + 1$.

— Partie 3 —

$2-2-2$ isogénies et familles de courbes hyperelliptiques

La situation

Genre 1 Problème classique des 2-isogénies entre courbes elliptiques.

Genre 2 Construction connue depuis Richelot (19^{e} siècle). Formules explicites données par Bost et Mestre.

Genre 3 Smith a donné des exemples de courbes hyperelliptiques en genre 3 qui sont $2-2-2$ isogènes grâce à l'existence d'une factorisation non triviale de $f(x)-g(z)$ conduisant à une correspondance entre les courbes hyperelliptiques $y^2=f(x)$ et $y^2=g(x)$.

Genre g Mestre donne des familles (de dimension $g+1$) de courbes hyperelliptiques de genre g avec une $\underbrace{2\cdots 2}_{g}$ isogénie.

La situation

Genre 1 Problème classique des 2-isogénies entre courbes elliptiques.

Genre 2 Construction connue depuis Richelot (19^{e} siècle). Formules explicites données par Bost et Mestre.

Genre 3 Smith a donné des exemples de courbes hyperelliptiques en genre 3 qui sont $2-2-2$ isogènes grâce à l'existence d'une factorisation non triviale de $f(x)-g(z)$ conduisant à une correspondance entre les courbes hyperelliptiques $y^2=f(x)$ et $y^2=g(x)$.

Genre g Mestre donne des familles (de dimension $g+1$) de courbes hyperelliptiques de genre g avec une $\underbrace{2\cdots 2}_{g}$ isogénie.

La situation

Genre 1 Problème classique des 2-isogénies entre courbes elliptiques.

Genre 2 Construction connue depuis Richelot (19^{e} siècle). Formules explicites données par Bost et Mestre.

Genre 3 Smith a donné des exemples de courbes hyperelliptiques en genre 3 qui sont $2-2-2$ isogènes grâce à l'existence d'une factorisation non triviale de $f(x)-g(z)$ conduisant à une correspondance entre les courbes hyperelliptiques $y^2=f(x)$ et $y^2=g(x)$.

Genre g Mestre donne des familles (de dimension $g+1$) de courbes hyperelliptiques de genre g avec une $\underbrace{2\cdots 2}_{g}$ isogénie.

La situation

Genre 1 Problème classique des 2-isogénies entre courbes elliptiques.

Genre 2 Construction connue depuis Richelot (19^{e} siècle). Formules explicites données par Bost et Mestre.

Genre 3 Smith a donné des exemples de courbes hyperelliptiques en genre 3 qui sont $2-2-2$ isogènes grâce à l'existence d'une factorisation non triviale de $f(x)-g(z)$ conduisant à une correspondance entre les courbes hyperelliptiques $y^2=f(x)$ et $y^2=g(x)$.

Genre g Mestre donne des familles (de dimension $g+1$) de courbes hyperelliptiques de genre g avec une $\underbrace{2\cdots 2}_{g}$ isogénie.

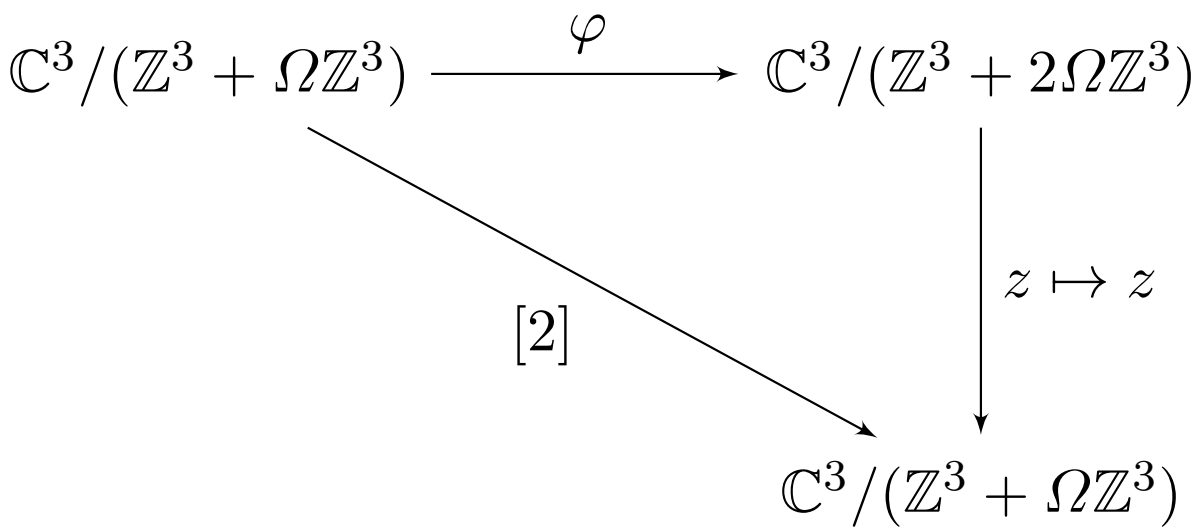
La situation

But (première partie)

Trouver toutes les courbes hyperelliptiques de genre 3 pour lesquelles il y a une courbe hyperelliptique et une $2-2-2$ isogénie entre leurs jacobiennes.

Factorisation de la multiplication par 2

On peut factoriser la multiplication par 2 par

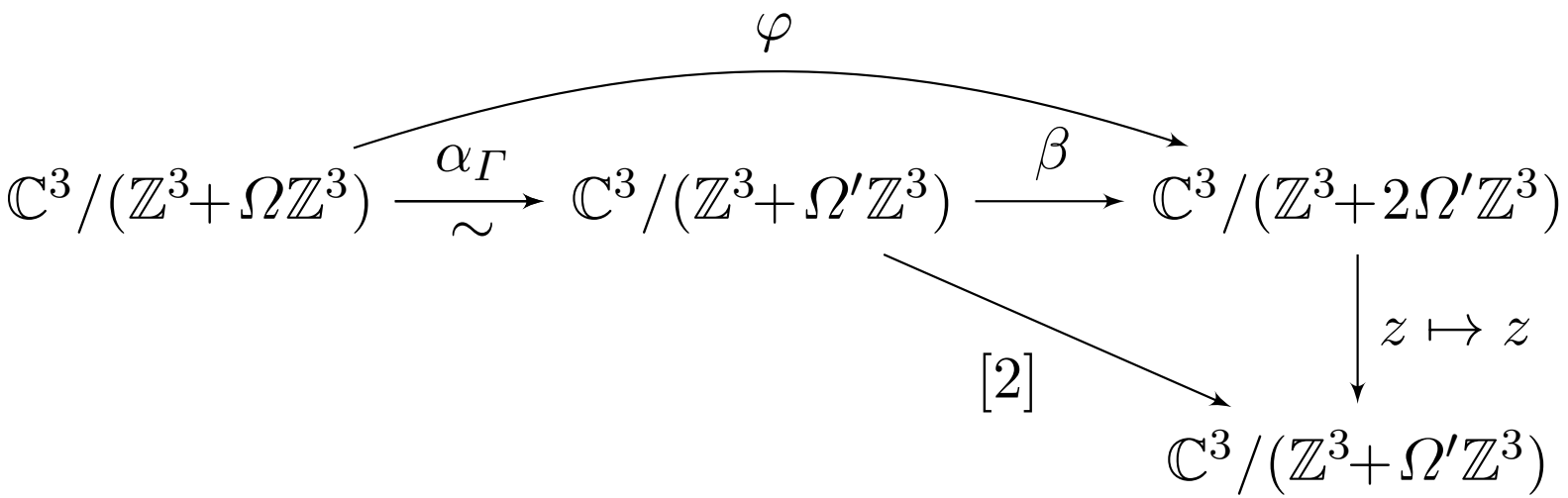


où la $2-2-2$ isogénie φ est donnée par

$$\begin{array}{rccc} \varphi : & \mathbb{C}^3/(\mathbb{Z}^3+\Omega\mathbb{Z}^3) & \longrightarrow & \mathbb{C}^3/(\mathbb{Z}^3+2\Omega\mathbb{Z}^3) \\ & z & \longmapsto & 2z \end{array}$$

Factorisation de la multiplication par 2

Pour le cas général, on utilise l'action de $\mathrm{Sp}_6(\mathbb{Z})$:



avec

$$\Omega' = \Gamma \cdot \Omega = (A\Omega + B)(C\Omega + D)^{-1}$$

$$\begin{array}{rccc} \alpha_\Gamma : & \mathbb{C}^3/(\mathbb{Z}^3 + \Omega\mathbb{Z}^3) & \longrightarrow & \mathbb{C}^3/(\mathbb{Z}^3 + \Omega'\mathbb{Z}^3) \\ & z & \longmapsto & {}^t(C\Omega + D)^{-1} z \end{array}$$

l'action $\mathrm{Sp}_6(\mathbb{Z})$.

Stratégie

- On part de Ω périodes de $\mathrm{Jac}(y^2 = \prod_{i=1}^{8}(x - x_i))$.
- On veut une condition sur les x_i pour que $\mathbb{C}^3/(\mathbb{Z}^3 + 2\Omega'\mathbb{Z}^3)$ soit la jacobienne d'une courbe hyperelliptique.
- On dispose de plusieurs outils :
  - L'annulation d'une thêta constante paire.
  - La formule de Thomae qui permet d'exprimer les thêta constantes en fonction des x_i.
  - La formule de duplication pour passer des thêta de Ω à 2Ω.
  - L'équation fonctionnelle (on donne une généralisation) qui permet de passer de Ω à Ω'.
- Pour étudier l'action de Sp_6, on classifie les isogénies suivant leur noyau. (Les points de Weierstrass sont d'ordre 2).

Stratégie

- On part de Ω périodes de $\mathrm{Jac}(y^2 = \prod_{i=1}^{8}(x - x_i))$.
- On veut une condition sur les x_i pour que $\mathbb{C}^3/(\mathbb{Z}^3 + 2\Omega'\mathbb{Z}^3)$ soit la jacobienne d'une courbe hyperelliptique.
- On dispose de plusieurs outils :
  - L'annulation d'une thêta constante paire.
  - La formule de Thomae qui permet d'exprimer les thêta constantes en fonction des x_i.
  - La formule de duplication pour passer des thêta de Ω à 2Ω.
  - L'équation fonctionnelle (on donne une généralisation) qui permet de passer de Ω à Ω'.
- Pour étudier l'action de Sp_6, on classifie les isogénies suivant leur noyau. (Les points de Weierstrass sont d'ordre 2).

Stratégie

- On part de Ω périodes de $\mathrm{Jac}(y^2 = \prod_{i=1}^{8}(x - x_i))$.
- On veut une condition sur les x_i pour que $\mathbb{C}^3/(\mathbb{Z}^3 + 2\Omega'\mathbb{Z}^3)$ soit la jacobienne d'une courbe hyperelliptique.
- On dispose de plusieurs outils :
  - L'annulation d'une thêta constante paire.
  - La formule de Thomae qui permet d'exprimer les thêta constantes en fonction des x_i.
  - La formule de duplication pour passer des thêta de Ω à 2Ω.
  - L'équation fonctionnelle (on donne une généralisation) qui permet de passer de Ω à Ω'.
- Pour étudier l'action de Sp_6, on classifie les isogénies suivant leur noyau. (Les points de Weierstrass sont d'ordre 2).

Stratégie

- On part de Ω périodes de $\mathrm{Jac}(y^2 = \prod_{i=1}^{8}(x - x_i))$.
- On veut une condition sur les x_i pour que $\mathbb{C}^3/(\mathbb{Z}^3 + 2\Omega'\mathbb{Z}^3)$ soit la jacobienne d'une courbe hyperelliptique.
- On dispose de plusieurs outils :
  - L'annulation d'une thêta constante paire.
  - La formule de Thomae qui permet d'exprimer les thêta constantes en fonction des x_i.
  - La formule de duplication pour passer des thêta de Ω à 2Ω.
  - L'équation fonctionnelle (on donne une généralisation) qui permet de passer de Ω à Ω'.
- Pour étudier l'action de Sp_6, on classifie les isogénies suivant leur noyau. (Les points de Weierstrass sont d'ordre 2).

Stratégie

- On part de Ω périodes de $\mathrm{Jac}(y^2 = \prod_{i=1}^{8}(x - x_i))$.
- On veut une condition sur les x_i pour que $\mathbb{C}^3/(\mathbb{Z}^3 + 2\Omega'\mathbb{Z}^3)$ soit la jacobienne d'une courbe hyperelliptique.
- On dispose de plusieurs outils :
  - L'annulation d'une thêta constante paire.
  - La formule de Thomae qui permet d'exprimer les thêta constantes en fonction des x_i.
  - La formule de duplication pour passer des thêta de Ω à 2Ω.
  - L'équation fonctionnelle (on donne une généralisation) qui permet de passer de Ω à Ω'.
- Pour étudier l'action de Sp_6, on classifie les isogénies suivant leur noyau. (Les points de Weierstrass sont d'ordre 2).

Stratégie

- On part de Ω périodes de $\mathrm{Jac}(y^2 = \prod_{i=1}^{8}(x - x_i))$.
- On veut une condition sur les x_i pour que $\mathbb{C}^3/(\mathbb{Z}^3 + 2\Omega'\mathbb{Z}^3)$ soit la jacobienne d'une courbe hyperelliptique.
- On dispose de plusieurs outils :
  - L'annulation d'une thêta constante paire.
  - La formule de Thomae qui permet d'exprimer les thêta constantes en fonction des x_i.
  - La formule de duplication pour passer des thêta de Ω à 2Ω.
  - L'équation fonctionnelle (on donne une généralisation) qui permet de passer de Ω à Ω'.
- Pour étudier l'action de Sp_6, on classifie les isogénies suivant leur noyau. (Les points de Weierstrass sont d'ordre 2).

Stratégie

- On part de Ω périodes de $\mathrm{Jac}(y^2 = \prod_{i=1}^{8}(x - x_i))$.
- On veut une condition sur les x_i pour que $\mathbb{C}^3/(\mathbb{Z}^3 + 2\Omega'\mathbb{Z}^3)$ soit la jacobienne d'une courbe hyperelliptique.
- On dispose de plusieurs outils :
  - L'annulation d'une thêta constante paire.
  - La formule de Thomae qui permet d'exprimer les thêta constantes en fonction des x_i.
  - La formule de duplication pour passer des thêta de Ω à 2Ω.
  - L'équation fonctionnelle (on donne une généralisation) qui permet de passer de Ω à Ω'.
- Pour étudier l'action de Sp_6, on classifie les isogénies suivant leur noyau. (Les points de Weierstrass sont d'ordre 2).

Stratégie

- On part de Ω périodes de $\mathrm{Jac}(y^2 = \prod_{i=1}^{8}(x - x_i))$.
- On veut une condition sur les x_i pour que $\mathbb{C}^3/(\mathbb{Z}^3 + 2\Omega'\mathbb{Z}^3)$ soit la jacobienne d'une courbe hyperelliptique.
- On dispose de plusieurs outils :
  - L'annulation d'une thêta constante paire.
  - La formule de Thomae qui permet d'exprimer les thêta constantes en fonction des x_i.
  - La formule de duplication pour passer des thêta de Ω à 2Ω.
  - L'équation fonctionnelle (on donne une généralisation) qui permet de passer de Ω à Ω'.
- Pour étudier l'action de Sp_6, on classifie les isogénies suivant leur noyau. (Les points de Weierstrass sont d'ordre 2).

Les noyaux : deux configurations géométriques

Pour déterminer toutes les courbes, on commence par caractériser les noyaux possibles. Ils doivent être

- isomorphes à $(\mathbb{Z}/2\mathbb{Z})^3$,
- totalement isotropes pour le pairing de Weil modulo 2.

Proposition

Il y a 135 tels sous groupes.

Toutefois ils ne correspondent qu'à deux configurations distinctes.

- 105 groupes « tractables » *i.e.* engendrés par des différences de 2 points,
- 30 groupes en « disposition de Fano ».

Les noyaux : deux configurations géométriques

Pour déterminer toutes les courbes, on commence par caractériser les noyaux possibles. Ils doivent être

- isomorphes à $(\mathbb{Z}/2\mathbb{Z})^3$,
- totalement isotropes pour le pairing de Weil modulo 2.

Proposition

Il y a 135 tels sous groupes.

Toutefois ils ne correspondent qu'à deux configurations distinctes.

- 105 groupes « tractables » *i.e.* engendrés par des différences de 2 points,
- 30 groupes en « disposition de Fano ».

Les noyaux : deux configurations géométriques

Pour déterminer toutes les courbes, on commence par caractériser les noyaux possibles. Ils doivent être

- isomorphes à $(\mathbb{Z}/2\mathbb{Z})^3$,
- totalement isotropes pour le pairing de Weil modulo 2.

Proposition

Il y a 135 tels sous groupes.

Toutefois ils ne correspondent qu'à deux configurations distinctes.

- 105 groupes « tractables » *i.e.* engendrés par des différences de 2 points,
- 30 groupes en « disposition de Fano ».

Les noyaux : deux configurations géométriques

Pour déterminer toutes les courbes, on commence par caractériser les noyaux possibles. Ils doivent être

- isomorphes à $(\mathbb{Z}/2\mathbb{Z})^3$,
- totalement isotropes pour le pairing de Weil modulo 2.

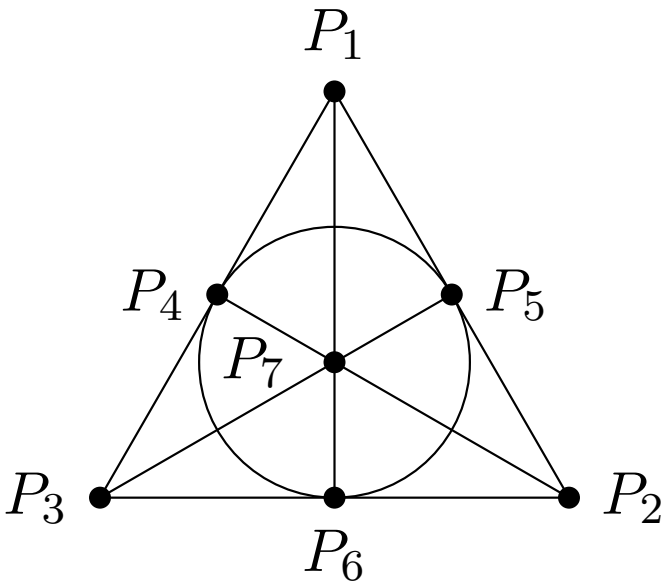
Proposition

Il y a 135 tels sous groupes.

Toutefois ils ne correspondent qu'à deux configurations distinctes.

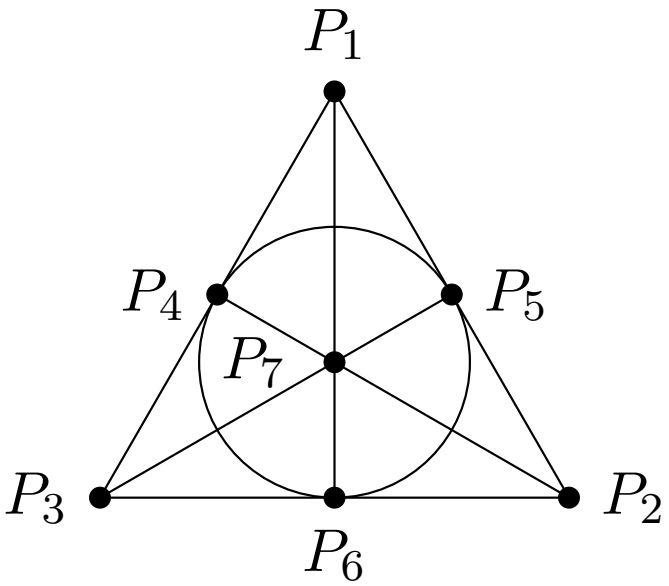
- 105 groupes « tractables » *i.e.* engendrés par des différences de 2 points,
- 30 groupes en « disposition de Fano ».

La « disposition de Fano »



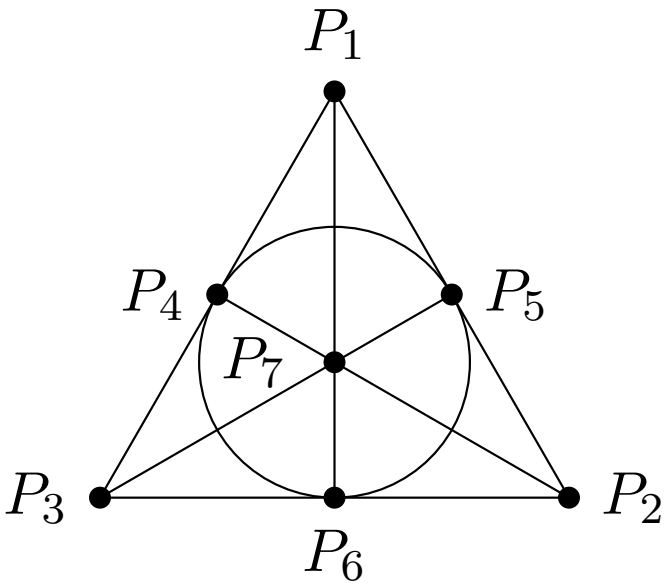
- P_8 n'est pas représenté : les éléments sont les 7 droites et l'ensemble vide modulo complémentaire.
- Les 7 droites sont d'ordre 2.
- L'addition de deux droites est donnée par la troisième droite possédant un point commun.

La « disposition de Fano »



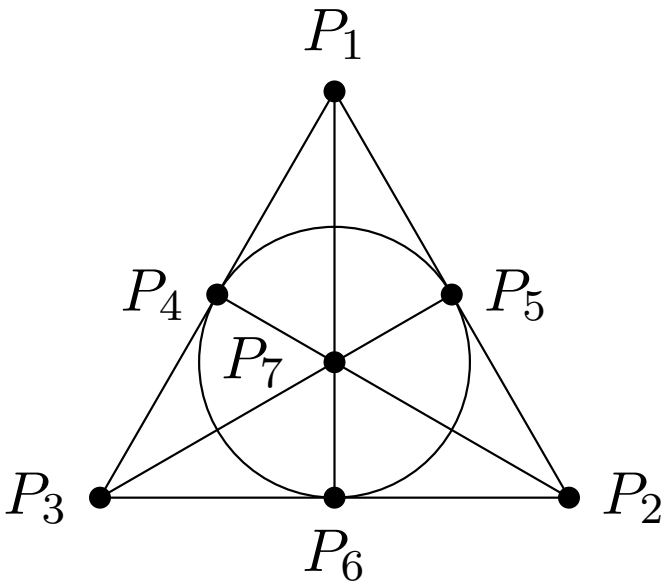
- P_8 n'est pas représenté : les éléments sont les 7 droites et l'ensemble vide modulo complémentaire.
- Les 7 droites sont d'ordre 2.
- L'addition de deux droites est donnée par la troisième droite possédant un point commun.

La « disposition de Fano »



- P_8 n'est pas représenté : les éléments sont les 7 droites et l'ensemble vide modulo complémentaire.
- Les 7 droites sont d'ordre 2.
- L'addition de deux droites est donnée par la troisième droite possédant un point commun.

La « disposition de Fano »



- P_8 n'est pas représenté : les éléments sont les 7 droites et l'ensemble vide modulo complémentaire.
- Les 7 droites sont d'ordre 2.
- L'addition de deux droites est donnée par la troisième droite possédant un point commun.

Les quatre familles

Noyaux « tractables »

- Un famille *(f-1)* : c'est le genre 3 de la famille de Mestre, donnée par

$$\text{“Trace”}_{\mathfrak{S}_3 \hookrightarrow \mathfrak{S}_6}(x_1x_2x_3+x_1x_2x_4) = \sum_{\sigma \in \mathfrak{S}_3} \epsilon(\sigma)(x_1x_2x_3+x_1x_2x_4)^{\varphi(\sigma)}$$

où $\varphi(\sigma) \in \mathfrak{S}_6$ est « l'action » de σ sur les paires $(1,2)$, $(3,4)$ et $(5,6)$.

- Une famille *(f-2)* définie par un polynôme de degré total 16, 4 en chaque variable, ayant 19591 monômes. Le stabilisateur est $(\mathbb{Z}/2\mathbb{Z})^4 \rtimes \mathfrak{S}_4$, laissant invariant les transpositions (12), (34), (56) et (78) et agissant par $\mathfrak{S}_4$ sur ces paires.

Les quatre familles

Noyaux « tractables »

- Un famille *(f-1)* : c'est le genre 3 de la famille de Mestre, donnée par

$$\text{“Trace”}_{\mathfrak{S}_3 \hookrightarrow \mathfrak{S}_6}(x_1x_2x_3+x_1x_2x_4) = \sum_{\sigma \in \mathfrak{S}_3} \epsilon(\sigma)(x_1x_2x_3+x_1x_2x_4)^{\varphi(\sigma)}$$

où $\varphi(\sigma) \in \mathfrak{S}_6$ est « l'action » de σ sur les paires $(1,2)$, $(3,4)$ et $(5,6)$.

- Une famille *(f-2)* définie par un polynôme de degré total 16, 4 en chaque variable, ayant 19591 monômes. Le stabilisateur est $(\mathbb{Z}/2\mathbb{Z})^4 \rtimes \mathfrak{S}_4$, laissant invariant les transpositions (12), (34), (56) et (78) et agissant par $\mathfrak{S}_4$ sur ces paires.

Les quatre familles

Noyaux de « Fano »

- Une famille *(f-3)* : polynôme de 24 monômes, de degré total 4, linéaire en chaque variable :

$$\text{“Trace”}_{\mathfrak{S}_4 \hookrightarrow \mathfrak{S}_8}(x_1x_2x_5x_7) = \sum_{\sigma \in \mathfrak{S}_4} \epsilon(\sigma)(x_1x_2x_5x_7)^{\varphi(\sigma)}$$

  $\varphi(\sigma) \in \mathfrak{S}_8$, action conjointe de σ sur $\{1,2,3,4\}$ et $\{5,6,7,8\}$.

- Une famille *(f-4)* : un polynôme de degré total 24 et 6 en chaque variable, possédant 215601 monômes !

  Smith donne un exemple dans *(f-4)*. Soit $\alpha_7 = \frac{1+\sqrt{7}}{2} \in \mathbb{Q}(\sqrt{7})$. La famille, en t, de courbes

$$y^2 = \frac{x^7}{7} - \alpha_7 t x^5 - \alpha_7 t x^4 - (2\alpha_7+5)t^2x^3 - (4\alpha_7+6)t^2x^2 + ((3\alpha_7-2)t^3 - (\alpha_7+3)t^2)x + \alpha_7 t^3.$$

  et leurs conjuguées ($\alpha_7 \mapsto \frac{2}{\alpha_7}$) ont des jacobiennes 2–2–2 isogènes.

Les quatre familles

Noyaux de « Fano »

- Une famille *(f-3)* : polynôme de 24 monômes, de degré total 4, linéaire en chaque variable :

$$\text{“Trace”}_{\mathfrak{S}_4 \hookrightarrow \mathfrak{S}_8}(x_1x_2x_5x_7) = \sum_{\sigma \in \mathfrak{S}_4} \epsilon(\sigma)(x_1x_2x_5x_7)^{\varphi(\sigma)}$$

  $\varphi(\sigma) \in \mathfrak{S}_8$, action conjointe de σ sur $\{1,2,3,4\}$ et $\{5,6,7,8\}$.

- Une famille *(f-4)* : un polynôme de degré total 24 et 6 en chaque variable, possédant 215601 monômes !

  Smith donne un exemple dans *(f-4)*. Soit $\alpha_7 = \frac{1+\sqrt{7}}{2} \in \mathbb{Q}(\sqrt{7})$. La famille, en t, de courbes

$$y^2 = \frac{x^7}{7} - \alpha_7 t x^5 - \alpha_7 t x^4 - (2\alpha_7+5)t^2x^3 - (4\alpha_7+6)t^2x^2 + ((3\alpha_7-2)t^3 - (\alpha_7+3)t^2)x + \alpha_7 t^3.$$

  et leurs conjuguées ($\alpha_7 \mapsto \frac{2}{\alpha_7}$) ont des jacobiennes 2–2–2 isogènes.

Les quatre familles

Noyaux de « Fano »

- Une famille *(f-3)* : polynôme de 24 monômes, de degré total 4, linéaire en chaque variable :

$$\text{“Trace”}_{\mathfrak{S}_4 \hookrightarrow \mathfrak{S}_8}(x_1x_2x_5x_7) = \sum_{\sigma \in \mathfrak{S}_4} \epsilon(\sigma)(x_1x_2x_5x_7)^{\varphi(\sigma)}$$

  $\varphi(\sigma) \in \mathfrak{S}_8$, action conjointe de σ sur $\{1,2,3,4\}$ et $\{5,6,7,8\}$.

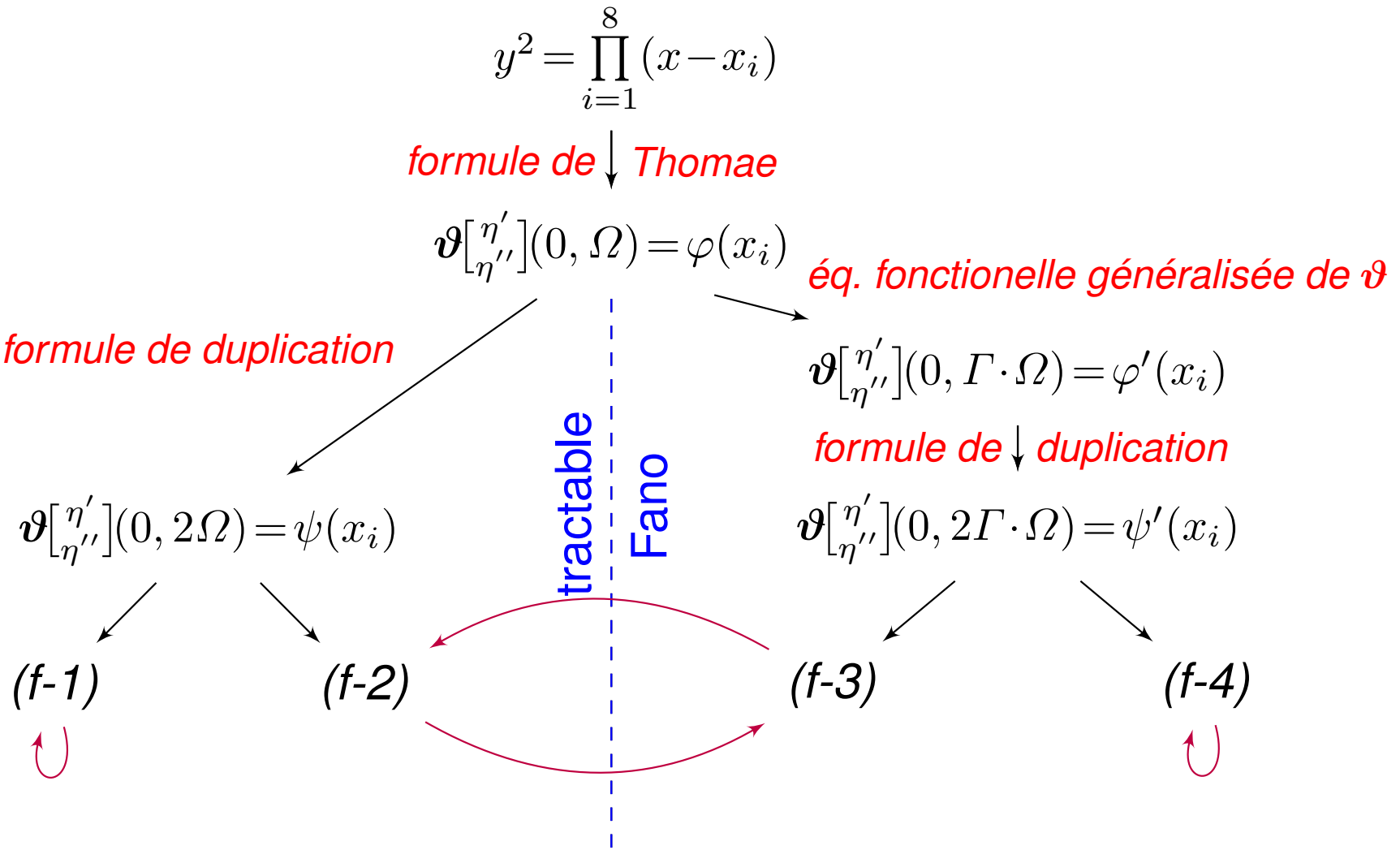
- Une famille *(f-4)* : un polynôme de degré total 24 et 6 en chaque variable, possédant 215601 monômes !

  Smith donne un exemple dans *(f-4)*. Soit $\alpha_7 = \frac{1+\sqrt{7}}{2} \in \mathbb{Q}(\sqrt{7})$. La famille, en t, de courbes

$$y^2 = \frac{x^7}{7} - \alpha_7 t x^5 - \alpha_7 t x^4 - (2\alpha_7+5)t^2x^3 - (4\alpha_7+6)t^2x^2 + ((3\alpha_7-2)t^3 - (\alpha_7+3)t^2)x + \alpha_7 t^3.$$

  et leurs conjuguées ($\alpha_7 \mapsto \frac{2}{\alpha_7}$) ont des jacobiennes 2–2–2 isogènes.

Résumé de la situation



Courbes tractables et de Fano

But (de la seconde partie)

Trouver des équations des courbes « tractables » de la famille (f-2), puis celles de « Fano » de la famille (f-3) et enfin une correspondance entre elles.

Construction trigonale de Recillas

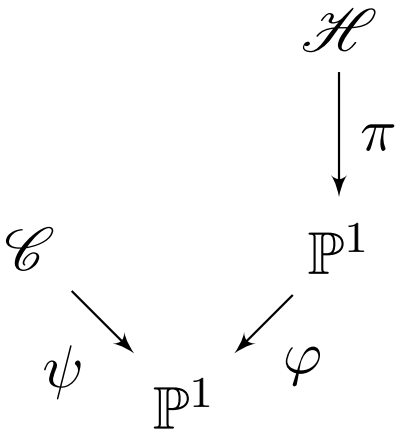


Diagramme de la construction trigonale

Construction trigonale de Recillas

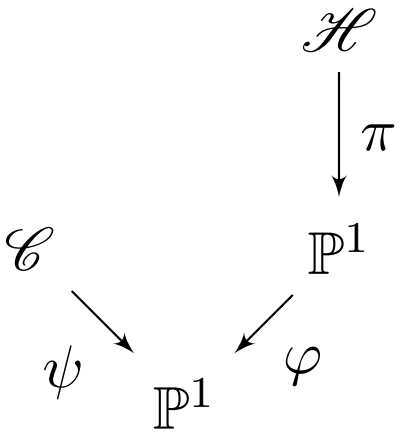


Diagramme de la construction trigonale

- π est un recouvrement de degré 2, φ est de degré 3 et ψ est de degré 4.
- L'application φ identifie les paires de points de Weierstrass.

Proposition

Il y a une $3-2$ correspondance entre $\mathscr{C}$ et $\mathscr{H}$ qui induit une $2-2-2$ isogénie entre leurs jacobiennes.

Construction trigonale de Recillas

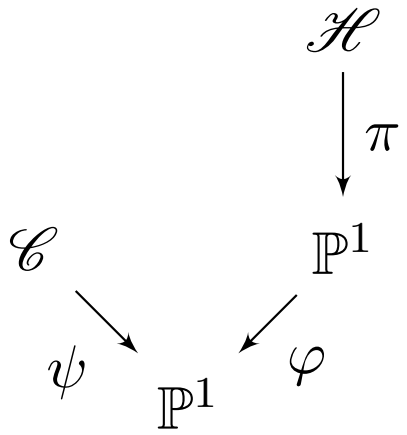


Diagramme de la construction trigonale

- π est un recouvrement de degré 2, φ est de degré 3 et ψ est de degré 4.
- L'application φ identifie les paires de points de Weierstrass.

Proposition

Il y a une $3-2$ correspondance entre $\mathscr{C}$ et $\mathscr{H}$ qui induit une $2-2-2$ isogénie entre leurs jacobiennes.

Construction trigonale de Recillas

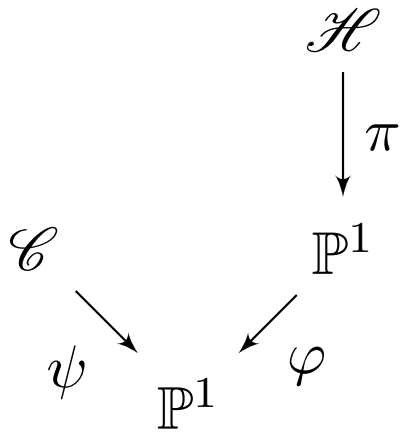


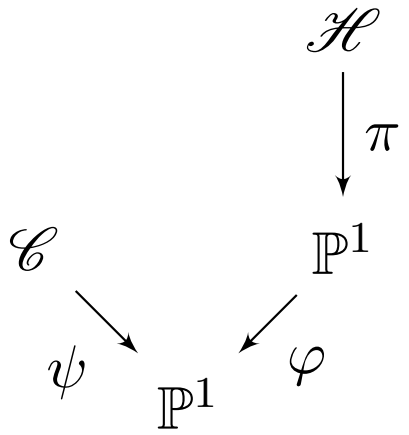
Diagramme de la construction trigonale

- π est un recouvrement de degré 2, φ est de degré 3 et ψ est de degré 4.
- L'application φ identifie les paires de points de Weierstrass.

Proposition

Il y a une $3-2$ correspondance entre $\mathscr{C}$ et $\mathscr{H}$ qui induit une $2-2-2$ isogénie entre leurs jacobiennes.

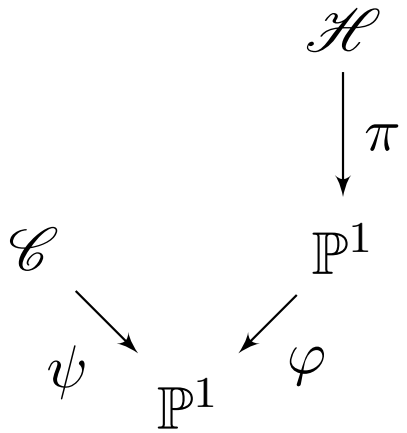
Construction trigonale de Recillas



Paramétrisation

- Plus facile de paramétrer $\mathscr{H}$ que de calculer φ.
- Par homographies, on choisit $P(x)=x^2+bx+c$ et
  - $\varphi(x)=\frac{xP(x)}{P(x)+a(x-1)(x-d)}$ et l'équation de $\mathscr{H}$:
  - $y^2=P(x)\big(P(x)+a(x-1)(x-d)\big)\big(P(x)-a(x-d)\big)\Big(f_2(x)\frac{\varphi(x)-\varphi(e)}{x-e}\Big)$.
- φ identifie les paires de points de Weierstrass à $0, \infty, 1$ et e.
- Génériquement, il y a une autre trigonale sauf si $d=e$.

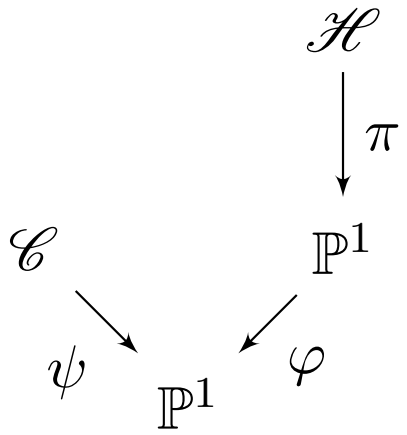
Construction trigonale de Recillas



Paramétrisation

- Plus facile de paramétrer $\mathscr{H}$ que de calculer φ.
- Par homographies, on choisit $P(x)=x^2+bx+c$ et
  - $\varphi(x)=\frac{xP(x)}{P(x)+a(x-1)(x-d)}$ et l'équation de $\mathscr{H}$:
  - $y^2=P(x)\big(P(x)+a(x-1)(x-d)\big)\big(P(x)-a(x-d)\big)\Big(f_2(x)\frac{\varphi(x)-\varphi(e)}{x-e}\Big)$.
- φ identifie les paires de points de Weierstrass à $0, \infty, 1$ et e.
- Génériquement, il y a une autre trigonale sauf si $d=e$.

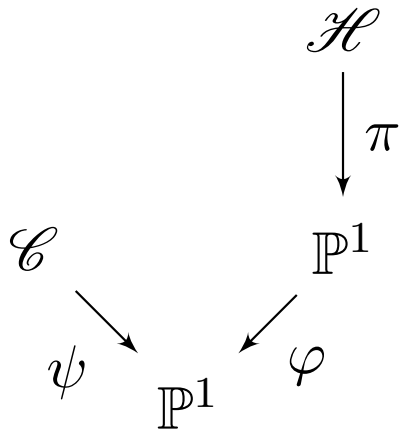
Construction trigonale de Recillas



Paramétrisation

- Plus facile de paramétrer $\mathscr{H}$ que de calculer φ.
- Par homographies, on choisit $P(x)=x^2+bx+c$ et
  - $\varphi(x)=\frac{xP(x)}{P(x)+a(x-1)(x-d)}$ et l'équation de $\mathscr{H}$:
  - $y^2=P(x)\big(P(x)+a(x-1)(x-d)\big)\big(P(x)-a(x-d)\big)\Big(f_2(x)\frac{\varphi(x)-\varphi(e)}{x-e}\Big)$.
- φ identifie les paires de points de Weierstrass à $0, \infty, 1$ et e.
- Génériquement, il y a une autre trigonale sauf si $d=e$.

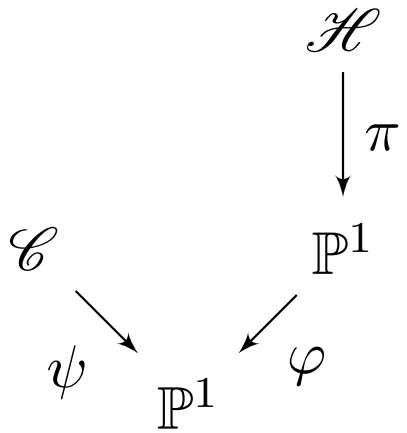
Construction trigonale de Recillas



Paramétrisation

- Plus facile de paramétrer $\mathscr{H}$ que de calculer φ.
- Par homographies, on choisit $P(x)=x^2+bx+c$ et
  - $\varphi(x)=\frac{xP(x)}{P(x)+a(x-1)(x-d)}$ et l'équation de $\mathscr{H}$:
  - $y^2=P(x)\big(P(x)+a(x-1)(x-d)\big)\big(P(x)-a(x-d)\big)\left(f_2(x)\frac{\varphi(x)-\varphi(e)}{x-e}\right)$.
- φ identifie les paires de points de Weierstrass à $0, \infty, 1$ et e.
- Génériquement, il y a une autre trigonale sauf si $d=e$.

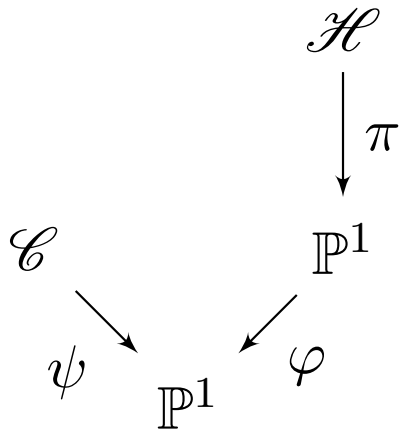
Construction trigonale de Recillas



Paramétrisation

- Plus facile de paramétrer $\mathscr{H}$ que de calculer φ.
- Par homographies, on choisit $P(x)=x^2+bx+c$ et
  - $\varphi(x)=\frac{xP(x)}{P(x)+a(x-1)(x-d)}$ et l'équation de $\mathscr{H}$:
  - $y^2=P(x)\big(P(x)+a(x-1)(x-d)\big)\big(P(x)-a(x-d)\big)\left(f_2(x)\frac{\varphi(x)-\varphi(e)}{x-e}\right)$.
- φ identifie les paires de points de Weierstrass à $0, \infty, 1$ et e.
- Génériquement, il y a une autre trigonale sauf si $d=e$.

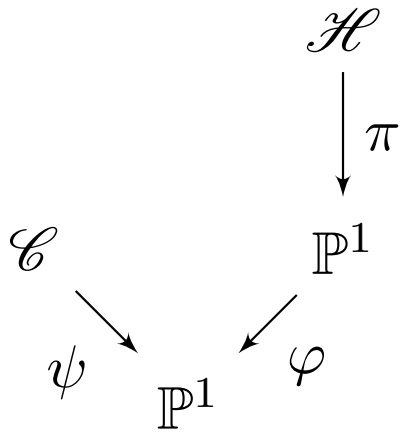
Construction trigonale de Recillas



Paramétrisation

- Plus facile de paramétrer $\mathscr{H}$ que de calculer φ.
- Par homographies, on choisit $P(x)=x^2+bx+c$ et
  - $\varphi(x)=\frac{xP(x)}{P(x)+a(x-1)(x-d)}$ et l'équation de $\mathscr{H}$:
  - $y^2=P(x)\big(P(x)+a(x-1)(x-d)\big)\big(P(x)-a(x-d)\big)\left(f_2(x)\frac{\varphi(x)-\varphi(e)}{x-e}\right)$.
- φ identifie les paires de points de Weierstrass à $0, \infty, 1$ et e.
- Génériquement, il y a une autre trigonale sauf si $d=e$.

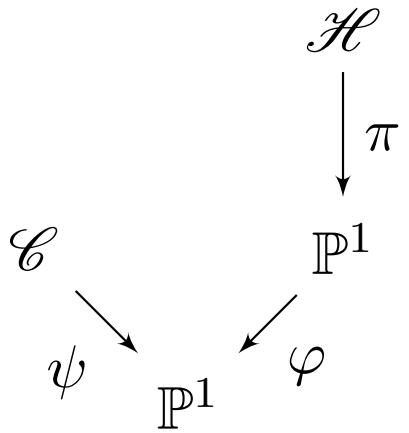
Construction trigonale de Recillas



Équation de $\mathscr{C}$

- Pour $Q \in \mathscr{C}$, on pose $T = \psi(Q)$ et $P_1, P_2, P_3 \in \mathscr{H}$ tel que
$$\varphi \circ \pi(P_i) = T = \psi(Q) = \varphi \circ \pi(\imath(P_i)).$$
- On interpole $\big(\pi(P_i), h(\pi(P_i))\big)$ avec $h(x) = \Lambda \frac{x+V}{x+W}$.
- On a deux copies de $\mathscr{C}$:
$$\Lambda^2 (x+V)^2 = (x+W)^2 f(x) \mod T f_2(x) - x f_1(x).$$
- On fait $U = V^2$ et on élimine U, W dans les coefficients en x.

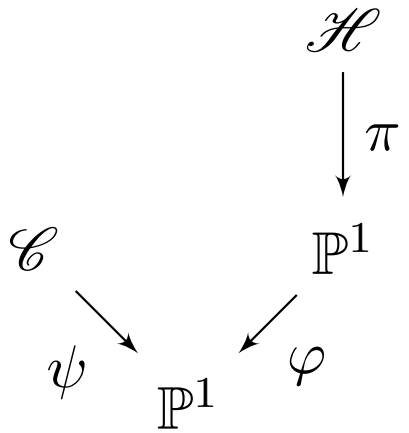
Construction trigonale de Recillas



Équation de $\mathscr{C}$

- Pour $Q \in \mathscr{C}$, on pose $T = \psi(Q)$ et $P_1, P_2, P_3 \in \mathscr{H}$ tel que
$$\varphi \circ \pi(P_i) = T = \psi(Q) = \varphi \circ \pi(\iota(P_i)).$$
- On interpole $\big(\pi(P_i), h(\pi(P_i))\big)$ avec $h(x) = \Lambda \frac{x+V}{x+W}$.
- On a deux copies de $\mathscr{C}$:
$$\Lambda^2 (x+V)^2 = (x+W)^2 f(x) \mod T f_2(x) - x f_1(x).$$
- On fait $U = V^2$ et on élimine U, W dans les coefficients en x.

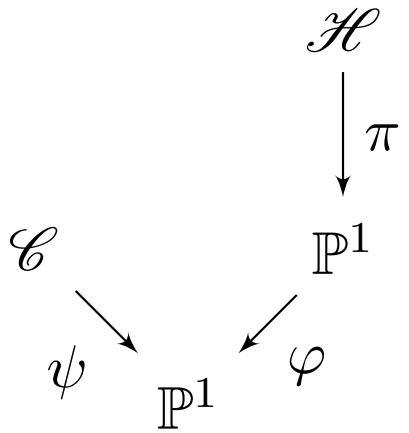
Construction trigonale de Recillas



Équation de $\mathscr{C}$

- Pour $Q \in \mathscr{C}$, on pose $T = \psi(Q)$ et $P_1, P_2, P_3 \in \mathscr{H}$ tel que
$$\varphi \circ \pi(P_i) = T = \psi(Q) = \varphi \circ \pi(\iota(P_i)).$$
- On interpole $\big(\pi(P_i), h(\pi(P_i))\big)$ avec $h(x) = \Lambda \frac{x+V}{x+W}$.
- On a deux copies de $\mathscr{C}$:
$$\Lambda^2(x+V)^2 = (x+W)^2 f(x) \mod T f_2(x) - x f_1(x).$$
- On fait $U = V^2$ et on élimine U, W dans les coefficients en x.

Construction trigonale de Recillas



Équation de $\mathscr{C}$

- Pour $Q \in \mathscr{C}$, on pose $T = \psi(Q)$ et $P_1, P_2, P_3 \in \mathscr{H}$ tel que
$$\varphi \circ \pi(P_i) = T = \psi(Q) = \varphi \circ \pi(\iota(P_i)).$$
- On interpole $\big(\pi(P_i), h(\pi(P_i))\big)$ avec $h(x) = \Lambda \frac{x+V}{x+W}$.
- On a deux copies de $\mathscr{C}$:
$$\Lambda^2(x+V)^2 = (x+W)^2 f(x) \mod T f_2(x) - x f_1(x).$$
- On fait $U = V^2$ et on élimine U, W dans les coefficients en x.

Famille *(f-3)*

Théorème

On a les énoncés équivalents.

1. *La courbe $\mathscr{C}$ est hyperelliptique .*
2. *Il y a une unique trigonale (i.e. $d = e$).*
3. *La courbe $\mathscr{H}$ appartient à la famille (f-2).*

Remarque

S'il n'y a aucune trigonale, $\mathscr{H}$ est une courbe de la famille (f-1) de Mestre.

Famille *(f-3)*

Théorème

On a les énoncés équivalents.

1. *La courbe $\mathscr{C}$ est hyperelliptique .*
2. *Il y a une unique trigonale (i.e. $d = e$).*
3. *La courbe $\mathscr{H}$ appartient à la famille (f-2).*

Remarque

S'il n'y a aucune trigonale, $\mathscr{H}$ est une courbe de la famille (f-1) de Mestre.

Le noyau de l'isogénie duale

Avec la $3-2$ correspondance, on peut calculer le noyau de *l'isogénie duale* entre $\mathrm{Jac}\,\mathscr{C}$ et $\mathrm{Jac}\,\mathscr{H}$.

Proposition

Le noyau est de type « Fano » : la courbe $\mathscr{C}$ est dans la famille (f-3) ou (f-4).

Le noyau de l'isogénie duale

Avec la $3-2$ correspondance, on peut calculer le noyau de *l'isogénie duale* entre $\mathrm{Jac}\,\mathscr{C}$ et $\mathrm{Jac}\,\mathscr{H}$.

Proposition

Le noyau est de type « Fano » : la courbe $\mathscr{C}$ est dans la famille (f-3) ou (f-4).

Modèle de Weierstrass et corps de définition

On définit $[f,g](x)=f'(x)g(x)-f(x)g'(x)$ et soit f_1, f_2, f_3 et f_4 les 4 polynômes correspondant aux paires de points identifiées dans l'équation de $\mathscr{H}$.

Proposition (Corps de définition)

1. *Il existe une équation de Weierstrass de $\mathscr{C}$ au-dessus d'une conique définie sur le corps de base.*
2. *On a une équation de Weierstrass dans l'extension engendrée par $\sqrt{\mathrm{Res}_x(f_i,f_j)}$, de degré générique 8.*
   En particulier, il existe une équation de Weierstrass sur $\mathbb{P}^1$ si tous les $[f_i,f_j](x)$ sont scindés.

Modèle de Weierstrass et corps de définition

On définit $[f,g](x)=f'(x)g(x)-f(x)g'(x)$ et soit f_1, f_2, f_3 et f_4 les 4 polynômes correspondant aux paires de points identifiées dans l'équation de $\mathscr{H}$.

Proposition (Corps de définition)

1. *Il existe une équation de Weierstrass de $\mathscr{C}$ au-dessus d'une conique définie sur le corps de base.*
2. *On a une équation de Weierstrass dans l'extension engendrée par $\sqrt{\mathrm{Res}_x(f_i,f_j)}$, de degré générique 8.*
   En particulier, il existe une équation de Weierstrass sur $\mathbb{P}^1$ si tous les $[f_i,f_j](x)$ sont scindés.

Les équations

- Cette extension de corps peut être paramétrée par

$$a = \frac{A^2 - dB^2 + d + dC^2 - C^2 - d^2}{d(d-1)},$$
$$b = \frac{A^2 + 1 - B^2 - d^2}{d-1},$$
$$c = \frac{dB^2 + d^2 - d - A^2}{d-1}.$$

- Un modèle de Weierstrass est donné par

$$\mathscr{W}_1 := \infty \quad \mathscr{W}_2 := 0 \quad \mathscr{W}_3 := 1 \quad \mathscr{W}_4 := d$$
$$\mathscr{W}_5 := \frac{A+C+d}{B+C+1} \quad \mathscr{W}_6 := \frac{(B-C-1)d}{A-C-d} \quad \mathscr{W}_7 := \frac{Bd-Cd+A+C}{A+B-d+1} \quad \mathscr{W}_8 := \frac{(A+B+d-1)d}{Bd+Cd+A-C}.$$

$\mathscr{W}_1, \ldots, \mathscr{W}_4$ sont les 4 points fixés par la trigonale φ.

Les équations

- Cette extension de corps peut être paramétrée par

$$a = \frac{A^2 - dB^2 + d + dC^2 - C^2 - d^2}{d(d-1)},$$
$$b = \frac{A^2 + 1 - B^2 - d^2}{d-1},$$
$$c = \frac{dB^2 + d^2 - d - A^2}{d-1}.$$

- Un modèle de Weierstrass est donné par

$$\mathscr{W}_1 := \infty \quad \mathscr{W}_2 := 0 \quad \mathscr{W}_3 := 1 \quad \mathscr{W}_4 := d$$
$$\mathscr{W}_5 := \frac{A+C+d}{B+C+1} \quad \mathscr{W}_6 := \frac{(B-C-1)d}{A-C-d} \quad \mathscr{W}_7 := \frac{Bd-Cd+A+C}{A+B-d+1} \quad \mathscr{W}_8 := \frac{(A+B+d-1)d}{Bd+Cd+A-C}.$$

$\mathscr{W}_1, \ldots, \mathscr{W}_4$ sont les 4 points fixés par la trigonale φ.

Les équations

- Cette extension de corps peut être paramétrée par

$$a = \frac{A^2 - dB^2 + d + dC^2 - C^2 - d^2}{d(d-1)},$$
$$b = \frac{A^2 + 1 - B^2 - d^2}{d-1},$$
$$c = \frac{dB^2 + d^2 - d - A^2}{d-1}.$$

- Un modèle de Weierstrass est donné par

$$\mathscr{W}_1 := \infty \quad \mathscr{W}_2 := 0 \quad \mathscr{W}_3 := 1 \quad \mathscr{W}_4 := d$$
$$\mathscr{W}_5 := \frac{A+C+d}{B+C+1} \quad \mathscr{W}_6 := \frac{(B-C-1)d}{A-C-d} \quad \mathscr{W}_7 := \frac{Bd-Cd+A+C}{A+B-d+1} \quad \mathscr{W}_8 := \frac{(A+B+d-1)d}{Bd+Cd+A-C}.$$

$\mathscr{W}_1, \ldots, \mathscr{W}_4$ sont les 4 points fixés par la trigonale φ.

Caractérisation du modèle de Weierstrass de $\mathscr{C}$

Théorème (Caractérisation géométrique de la famille *(f-3)*)

1. *Les j-invariants associés à $\{\mathscr{W}_5, \ldots, \mathscr{W}_8\}$ et $\{\mathscr{W}_1, \ldots, \mathscr{W}_4\}$ sont **égaux**.*
2. *Une courbe hyperelliptique est dans (f-3) si et seulement si il y a une partition 4-4 de ses points de Weierstrass avec un **birapport commun**.*

Corollaire

Une courbe hyperelliptique $\mathscr{C}$ est dans la famille (f-3) si et seulement si elle apparaît dans une construction trigonale.

Caractérisation du modèle de Weierstrass de $\mathscr{C}$

Théorème (Caractérisation géométrique de la famille *(f-3)*)

1. *Les j-invariants associés à $\{\mathscr{W}_5, \ldots, \mathscr{W}_8\}$ et $\{\mathscr{W}_1, \ldots, \mathscr{W}_4\}$ sont **égaux**.*
2. *Une courbe hyperelliptique est dans (f-3) si et seulement si il y a une partition 4-4 de ses points de Weierstrass avec un **birapport commun**.*

Corollaire

Une courbe hyperelliptique $\mathscr{C}$ est dans la famille (f-3) si et seulement si elle apparaît dans une construction trigonale.

Caractérisation du modèle de Weierstrass de $\mathscr{C}$

Corollaire

1. *La courbe $\mathscr{C}$ peut être calculée à partir de $\mathscr{H}$ avec les 4 points de Weierstrass $(0, 1, d, \infty)$ fixés par φ, et par l'homographie*
$$\mathscr{J} : w \mapsto \frac{(\overline{x}_{1,3} + x_{3,4})w - d(\overline{x}_{1,4} + x_{3,4})}{(x_{1,4} + x_{3,4})w - (x_{1,3} + x_{3,4})}$$
où $x_{i,j}$ et $\overline{x}_{i,j}$ sont les racines $[f_i, f_j](x)$.
2. *Réciproquement, si $\infty, 0, 1, \lambda_4, \ldots \lambda_8$ sont les points de Weierstrass de $\mathscr{C}$,*
$$A = -\frac{(\lambda_5\lambda_6 - \lambda_6\lambda_7 - \lambda_5 + \lambda_6)(\lambda_4 - 1)\lambda_4}{\lambda_4\lambda_5\lambda_6 - \lambda_4\lambda_6\lambda_7 - \lambda_4\lambda_6 + \lambda_4\lambda_7 - \lambda_5\lambda_7 + \lambda_6\lambda_7}$$
$$B = \frac{(\lambda_4 - 1)(\lambda_4\lambda_5 - \lambda_4\lambda_7 - \lambda_5\lambda_7 + \lambda_6\lambda_7}{\lambda_4\lambda_5\lambda_6 - \lambda_4\lambda_6\lambda_7 - \lambda_4\lambda_6 + \lambda_4\lambda_7 - \lambda_5\lambda_7 + \lambda_6\lambda_7}$$
$$C = \frac{(\lambda_4\lambda_5 - \lambda_4\lambda_7 - \lambda_5\lambda_6 + \lambda_5\lambda_7 - \lambda_5 + \lambda_6)\lambda_4}{\lambda_4\lambda_5\lambda_6 - \lambda_4\lambda_6\lambda_7 - \lambda_4\lambda_6 + \lambda_4\lambda_7 - \lambda_5\lambda_7 + \lambda_6\lambda_7}$$
$$d = \lambda_4.$$

Correspondance et involution hyperelliptique

La $3-2$ correspondance donnée par la construction trigonale ne respecte pas les involutions hyperelliptiques. Cependant,

Théorème

Il existe, sur une extension de degré 8, une correspondance $4-3$ entre les modèles de Weierstrass de $\mathscr{H}$ et $\mathscr{C}$, qui respecte les involutions hyperelliptiques : il y a des polynômes $P(x,X)$ et $Q(x,X)$ tels que

$$\begin{cases} y^2 = f(x) & (\mathscr{H}) \\ 0 = P(x,X) & \\ yY = Q(x,X) & \\ Y^2 = F(X) & (\mathscr{C}), \end{cases}$$

où $\deg_x(P) = 4$ et $\deg_X(P) = 3$.

Correspondance et involution hyperelliptique

La $3-2$ correspondance donnée par la construction trigonale ne respecte pas les involutions hyperelliptiques. Cependant,

Théorème

Il existe, sur une extension de degré 8, une correspondance $4-3$ entre les modèles de Weierstrass de $\mathscr{H}$ et $\mathscr{C}$, qui respecte les involutions hyperelliptiques : il y a des polynômes $P(x,X)$ et $Q(x,X)$ tels que

$$\begin{cases} y^2 = f(x) & (\mathscr{H}) \\ 0 = P(x,X) & \\ yY = Q(x,X) & \\ Y^2 = F(X) & (\mathscr{C}), \end{cases}$$

où $\deg_x(P) = 4$ et $\deg_X(P) = 3$.

Description de la correspondance

Proposition

Cette correspondance associe aux points de Weierstrass $0, 1, d$, et ∞ de $\mathscr{C}$, une paire de points de Weierstrass de $\mathscr{H}$.
Pour les points $\mathscr{W}_5, \ldots, \mathscr{W}_8$, elle associe 0 ou 2 paires de points de Weierstrass de $\mathscr{H}$.

Plus précisément, il y a des constantes telles que

$$P(x,0) = \lambda_1(x+\lambda_2)^2 f_4(x) \qquad P(x,1) = \lambda_3 f_2(x)$$
$$P(x,d) = \lambda_4(x+\lambda_5)^2 f_1(x) \qquad P(x,\infty) = \lambda_6(x+\lambda_7)^2 f_3(x)$$

et

$$P(x,\mathscr{W}_5) = \lambda_8 f_1 f_4 \qquad P(x,\mathscr{W}_6) = \lambda_9 f_1 f_4$$
$$P(x,\mathscr{W}_7) = \lambda_{10}(x^2+\lambda_{11}x+\lambda_{12})^2 \qquad P(x,\mathscr{W}_8) = \lambda_{13} f_3 f_4$$

Description de la correspondance

Proposition

Cette correspondance associe aux points de Weierstrass $0, 1, d$, et ∞ de $\mathscr{C}$, une paire de points de Weierstrass de $\mathscr{H}$.
Pour les points $\mathscr{W}_5, \ldots, \mathscr{W}_8$, elle associe 0 ou 2 paires de points de Weierstrass de $\mathscr{H}$.

Plus précisément, il y a des constantes telles que

$$P(x,0) = \lambda_1(x+\lambda_2)^2 f_4(x) \qquad P(x,1) = \lambda_3 f_2(x)$$
$$P(x,d) = \lambda_4(x+\lambda_5)^2 f_1(x) \qquad P(x,\infty) = \lambda_6(x+\lambda_7)^2 f_3(x)$$

et

$$P(x,\mathscr{W}_5) = \lambda_8 f_1 f_4 \qquad P(x,\mathscr{W}_6) = \lambda_9 f_1 f_4$$
$$P(x,\mathscr{W}_7) = \lambda_{10}(x^2+\lambda_{11}x+\lambda_{12})^2 \qquad P(x,\mathscr{W}_8) = \lambda_{13} f_3 f_4$$

Variétés abéliennes et jacobiennes de courbes hyperelliptiques, en particulier à multiplication complexe

Ivan Boyer

Sous la direction de Jean-François Mestre
Université Paris Diderot

24 janvier 2014