Restrictions sur l'algèbre des endomorphismes d'une jacobienne hyperelliptique

Pip Goodman

Jacobiennes

Soit C une courbe (lisse, irréductible, projective), on peut y associer une variété abélienne, $\mathrm{Jac}(C)$ appelée la jacobienne de C.

De plus, pour chaque morphisme $C \to C'$, on en obtient un autre entre les jacobiennes $\mathrm{Jac}(C) \to \mathrm{Jac}(C')$.

Jacobiennes

Soit C une courbe (lisse, irréductible, projective), on peut y associer une variété abélienne, $\mathrm{Jac}(C)$ appelée la jacobienne de C.

De plus, pour chaque morphisme $C \to C'$, on en obtient un autre entre les jacobiennes $\mathrm{Jac}(C) \to \mathrm{Jac}(C')$.

Soient K un corps de nombres et $f \in K[x]$ une polynôme de degré $2g+1$ ou $2g+2$ avec des racines distinctes.
Alors l'équation $y^2 = f(x)$ détermine une courbe de genre g.
On appelle une telle courbe *hyperelliptique*.

Notation

On écrit J_f pour la jacobienne d'une courbe hyperelliptique.

Notations

Représentations galoisennes

ℓ-torsion

Soit ℓ un nombre premier, on a une représentation

$$G_K := \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(J_f[\ell]).$$

Où $J_f[\ell]$ désigne les points d'ordre ℓ dans $J(\bar{K})$. Il est un espace vectoriel de dimension $2g$ sur $\mathbb{F}_\ell$.
On a $K(J_f[2]) = K(f)$, le corps de décomposition de f.

Représentations galoisennes

ℓ-torsion

Soit ℓ un nombre premier, on a une représentation

$$G_K := \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(J_f[\ell]).$$

Où $J_f[\ell]$ désigne les points d'ordre ℓ dans $J(\bar{K})$. Il est un espace vectoriel de dimension $2g$ sur $\mathbb{F}_\ell$.
On a $K(J_f[2]) = K(f)$, le corps de décomposition de f.

Question

Y a-t-il un rapport entre $\mathrm{End}(J_f)$ et les représentations ci-dessus / les corps $K(J_f[\ell])$?

En général, $K(f)$ n'a rien à voir avec $\mathrm{End}(J_f)$. Par exemple :

1. $f(x) = (x+1)(x^4+x^3+x^2+x+1)$, a $\mathrm{End}(J_f) \cong \mathbb{Z}$.
2. $f(x) = x(x^4+x^3+x^2+x+1)$, a $\mathrm{End}(J_f) \cong \mathbb{Z} \times \mathbb{Z}$.
3. $f(x) = (x-1)(x^4+x^3+x^2+x+1)$, a $\mathrm{End}(J_f) \cong \mathbb{Z}[\zeta_5]$.

Théorie de Galois inverse

Théorème (Serre '72)

Soit E/K une courbe elliptique avec $\mathrm{End}(E) \cong \mathbb{Z}$. Alors, pour presque tout nombres premiers ℓ, on a $\mathrm{Gal}(K(E[\ell])/K) = \mathrm{GL}_2(\mathbb{F}_\ell)$.

Théorème (Hall '08)

Soit $C_f : y^2 = f(x)$, où $\deg(f) = 2g + 1$. Soit $J_f = \mathrm{Jac}(C_f)$. Supposons que $\mathrm{End}(J_f) \cong \mathbb{Z}$, et f a une racine double modulo un nombre premier p. Alors, pour presque tout nombre premier ℓ, on a $\mathrm{Gal}(K(J_f[\ell])/K) = \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$.

Théorème (Zarhin '00)

Soit $f \in K[x]$ un polynôme de degré $n \geq 5$ tel que son groupe de Galois contient A_n. Alors l'anneau des endomorphismes de J_f est trivial.

Remarque

Il suffit de démontrer le résultat pour A_n.

Théorie de Galois inverse

Théorème (Serre '72)

Soit E/K une courbe elliptique avec $\mathrm{End}(E) \cong \mathbb{Z}$. Alors, pour presque tout nombres premiers ℓ, on a $\mathrm{Gal}(K(E[\ell])/K) = \mathrm{GL}_2(\mathbb{F}_\ell)$.

Théorème (Hall '08)

Soit $C_f : y^2 = f(x)$, où $\deg(f) = 2g + 1$. Soit $J_f = \mathrm{Jac}(C_f)$. Supposons que $\mathrm{End}(J_f) \cong \mathbb{Z}$, et f a une racine double modulo un nombre premier p. Alors, pour presque tout nombre premier ℓ, on a $\mathrm{Gal}(K(J_f[\ell])/K) = \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$.

Théorème (Zarhin '00)

Soit $f \in K[x]$ un polynôme de degré $n \geq 5$ tel que son groupe de Galois contient A_n. Alors l'anneau des endomorphismes de J_f est trivial.

Remarque

Il suffit de démontrer le résultat pour A_n.

Théorie de Galois inverse

Théorème (Serre '72)

Soit E/K une courbe elliptique avec $\mathrm{End}(E) \cong \mathbb{Z}$. Alors, pour presque tout nombres premiers ℓ, on a $\mathrm{Gal}(K(E[\ell])/K) = \mathrm{GL}_2(\mathbb{F}_\ell)$.

Théorème (Hall '08)

Soit $C_f : y^2 = f(x)$, où $\deg(f) = 2g + 1$. Soit $J_f = \mathrm{Jac}(C_f)$. Supposons que $\mathrm{End}(J_f) \cong \mathbb{Z}$, et f a une racine double modulo un nombre premier p. Alors, pour presque tout nombre premier ℓ, on a $\mathrm{Gal}(K(J_f[\ell])/K) = \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$.

Théorème (Zarhin '00)

Soit $f \in K[x]$ un polynôme de degré $n \geq 5$ tel que son groupe de Galois contient A_n. Alors l'anneau des endomorphismes de J_f est trivial.

Remarque

Il suffit de démontrer le résultat pour A_n.

Théorie de Galois inverse

Théorème (Serre '72)

Soit E/K une courbe elliptique avec $\mathrm{End}(E) \cong \mathbb{Z}$. Alors, pour presque tout nombres premiers ℓ, on a $\mathrm{Gal}(K(E[\ell])/K) = \mathrm{GL}_2(\mathbb{F}_\ell)$.

Théorème (Hall '08)

Soit $C_f : y^2 = f(x)$, où $\deg(f) = 2g + 1$. Soit $J_f = \mathrm{Jac}(C_f)$. Supposons que $\mathrm{End}(J_f) \cong \mathbb{Z}$, et f a une racine double modulo un nombre premier p. Alors, pour presque tout nombre premier ℓ, on a $\mathrm{Gal}(K(J_f[\ell])/K) = \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$.

Théorème (Zarhin '00)

Soit $f \in K[x]$ un polynôme de degré $n \geq 5$ tel que son groupe de Galois contient A_n. Alors l'anneau des endomorphismes de J_f est trivial.

Remarque

Il suffit de démontrer le résultat pour A_n.

Règles du jeu

Théorème (Zarhin '00)

Soit $f \in K[x]$ un polynôme de degré $n \geq 5$ tel que son groupe de Galois contient A_n. Alors l'anneau des endomorphismes de J_f est trivial.

Remarque

Il suffit de démontrer le résultat pour A_n.

Pour J_f/K, on a :

- $\mathrm{End}(J_f)$ est un $\mathbb{Z}$-module libre de rang $< 4g^2$.
- Les idempotents dans $\mathrm{End}(J_f)$ donnent lieu à des idempotents dans $\mathrm{End}(J_f) \otimes \mathbb{Z}/2\mathbb{Z}$.
- $G_K = \mathrm{Gal}(\bar{K}/K)$ agit sur $\mathrm{End}(J_f)$ par conjugaison.
- $\mathrm{End}(J_f) \otimes \mathbb{Z}/2\mathbb{Z}$ est une sous-algèbre de $\mathrm{End}(J_f[2])$.

Qu'est-ce que l'on peut dire pour des groupes de Galois plus petits ?

Zarhin a énormément travaillé là-dessus quand le groupe de Galois est grand et non-résoluble. Le "plus petit" qu'il a regardé est le suivant :

Théorème (Elkin, Zarhin '06,'08)

Soit $n = q + 1$, où $q \geq 5$ est une puissance d'un nombre premier et est congru à ± 3 ou 7 modulo 8. Supposons que $f(x) \in K[x]$ de degré n soit irréductible et $\mathrm{Gal}(f) \cong \mathrm{PSL}_2(\mathbb{F}_q)$. Alors, une des suivantes est vraie :

1. $\mathrm{End}^0(J_f) = \mathbb{Q}$ *ou un corps quadratique.*
2. $q \equiv 3 \mod 4$ *et* $\mathrm{End}^0(J_f) \cong M_g(\mathbb{Q}(\sqrt{-q}))$.

Un résultat de Lombardo

Théorème (Lombardo '19)

Soit $f \in K[x]$ un polynôme irréductible de degré 5. Alors $\mathrm{End}^0(J_f)$ est une algèbre à division.

Peut-on améliorer le résultat de Lombardo ?

Exemple

Il est facile de trouver des jacobiennes J_f avec $\mathrm{End}(J_f) \cong \mathbb{Z}$, donc voici d'autres exemples.

$\mathrm{Gal}(f)$	$\mathrm{End}(J_f)$	$f(x)$
F_5	$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	$x^5 + 10x^3 + 20x + 5$
F_5	$\mathbb{Z}[\zeta_5]$	$x^5 - 2$
D_5	$\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$	$x^5 - 19x^4 + 107x^3 + 95x^2 + 88x - 16$
F_5	R	$52x^5 + 104x^4 + 104x^3 + 52x^2 + 12x + 1$

où R est l'ordre maximal d'un corps de nombre à CM, défini par le polynôme $x^4 + x^3 + 2x^2 - 4x + 3$. On note que ce corps est cyclique ramifié seulement à 13, et 2 est totalement inerte.

On note aussi que lorsque $\mathrm{Gal}(f) \cong F_5$ et J_f est à CM, $\mathrm{End}^0(J_f)$ est isomorphe à l'unique extension de degré 4 de $\mathbb{Q}$ contenu dans $\mathbb{Q}(f)$.

Peut-on améliorer le résultat de Lombardo ?

Exemple

Il est facile de trouver des jacobiennes J_f avec $\mathrm{End}(J_f) \cong \mathbb{Z}$, donc voici d'autres exemples.

$\mathrm{Gal}(f)$	$\mathrm{End}(J_f)$	$f(x)$
F_5	$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	$x^5 + 10x^3 + 20x + 5$
F_5	$\mathbb{Z}[\zeta_5]$	$x^5 - 2$
D_5	$\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$	$x^5 - 19x^4 + 107x^3 + 95x^2 + 88x - 16$
F_5	R	$52x^5 + 104x^4 + 104x^3 + 52x^2 + 12x + 1$

où R est l'ordre maximal d'un corps de nombre à CM, défini par le polynôme $x^4 + x^3 + 2x^2 - 4x + 3$. On note que ce corps est cyclique ramifié seulement à 13, et 2 est totalement inerte.

On note aussi que lorsque $\mathrm{Gal}(f) \cong F_5$ et J_f est à CM, $\mathrm{End}^0(J_f)$ est isomorphe à l'unique extension de degré 4 de $\mathbb{Q}$ contenu dans $\mathbb{Q}(f)$.

Peut-on améliorer le résultat de Lombardo ?

Exemple

Il est facile de trouver des jacobiennes J_f avec $\mathrm{End}(J_f) \cong \mathbb{Z}$, donc voici d'autres exemples.

$\mathrm{Gal}(f)$	$\mathrm{End}(J_f)$	$f(x)$
F_5	$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	$x^5 + 10x^3 + 20x + 5$
F_5	$\mathbb{Z}[\zeta_5]$	$x^5 - 2$
D_5	$\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$	$x^5 - 19x^4 + 107x^3 + 95x^2 + 88x - 16$
F_5	R	$52x^5 + 104x^4 + 104x^3 + 52x^2 + 12x + 1$

où R est l'ordre maximal d'un corps de nombre à CM, défini par le polynôme $x^4 + x^3 + 2x^2 - 4x + 3$. On note que ce corps est cyclique ramifié seulement à 13, et 2 est totalement inerte.

On note aussi que lorsque $\mathrm{Gal}(f) \cong F_5$ et J_f est à CM, $\mathrm{End}^0(J_f)$ est isomorphe à l'unique extension de degré 4 de $\mathbb{Q}$ contenu dans $\mathbb{Q}(f)$.

Genre 2

Théorème (G. '21)

Soit $f(x) \in K[x]$ un polynôme de degré 5 ou 6, et supposons que $\mathrm{Gal}(f)$ contient un élément d'ordre 5. Alors, l'une des assertions suivantes est vérifiée :

1. $\mathrm{End}(J_f) \cong \mathbb{Z}$.
2. $\mathrm{End}(J_f) \cong \mathbb{Z}\left[\frac{1+r\sqrt{D}}{2}\right]$, *où* $D \equiv 5 \mod 8$, $D > 0$ *et* $2 \nmid r$.
3. $\mathrm{End}(J_f) \cong R$, *où R est un ordre maximal à 2 dans un corps à CM de degré 4, qui de plus est totalement inerte à 2.*

Remarque

En précisant $\mathrm{Gal}(f)$, on obtient plus d'informations sur $\mathrm{End}(J_f)$.

Genre ≥ 1

Théorème (G.'21)

Soit $f(x) \in K[x]$ un polynôme de degré $2g+1$ ou $2g+2$. Supposons que $\mathrm{Gal}(f)$ contient un élément d'ordre premier $p = 2g+1$, et g satisfait d'autres conditions. Alors l'une des assertions suivantes est vérifiée :

1. $\mathrm{End}^0(J_f)$ *est un corps de nombres, avec des restrictions sur les idéaux premiers au dessus de 2 ;*
2. $\mathrm{End}^0(J_f) \cong M_a(F)$ *où $F \subsetneq \mathbb{Q}(\zeta_p)$ est un corps à CM et $a = \frac{2g}{[F:\mathbb{Q}]}$.*

Satisfait par $g = 1, 2, 3, 5, 6, 9, 11, 14, 18, 23, 26, 29, 30, 33, 35, 39, 41, \ldots$

Genre ≥ 1

Théorème (G.'21)

Soit $f(x) \in K[x]$ un polynôme de degré $2g+1$ ou $2g+2$. Supposons que $\mathrm{Gal}(f)$ contient un élément d'ordre premier $p = 2g+1$, et g satisfait d'autres conditions. Alors l'une des assertions suivantes est vérifiée :

1. $\mathrm{End}^0(J_f)$ *est un corps de nombres, avec des restrictions sur les idéaux premiers au dessus de 2 ;*
2. $\mathrm{End}^0(J_f) \cong M_a(F)$ *où $F \subsetneq \mathbb{Q}(\zeta_p)$ est un corps à CM et $a = \frac{2g}{[F:\mathbb{Q}]}$.*

Satisfait par $g = 1, 2, 3, 5, 6, 9, 11, 14, 18, 23, 26, 29, 30, 33, 35, 39, 41, \ldots$

Idée de la démonstration

On considère le cas où l'action de $\mathrm{Gal}(f)$ sur $J[2]$ est irréductible. On peut supposer que $|\mathrm{Gal}(f)| = p$. D'abord on montre que $\mathrm{End}_K^0(J_f)$ est un corps.

Restrictions sur le corps des endomorphismes

Soit A/K une variété abélienne de dimension g. On écrit L/K pour l'extension minimale sur laquelle tous les endomorphismes de A sont défini.
E.g. $E : y^2 = x^3 - 2$ a $g = 1$ et $L = \mathbb{Q}(\zeta_3)$.

Théorème (G.'21)

Supposons que $p = 2g + 1$ est un nombre premier divisant $[L : K]$. Alors $\mathrm{End}^0(A) \cong M_a(F)$ où $F \subsetneq \mathbb{Q}(\zeta_p)$ est un corps à CM et $a = \frac{2g}{[F:\mathbb{Q}]}$.

Démonstration esquissée

Démonstration esquissée

1. D'abord on montre que $\mathrm{End}^0(A) \cong M_n(D)$ où D est une algèbre à division de dimension finie sur $\mathbb{Q}$ qui satisfait $[D : \mathbb{Q}]n \leq 2g = p - 1$ et $n > 1$.
2. On observe que l'action de $\mathrm{Gal}(L/K)$ sur $M_n(D)$ par automorphismes est fidèle.
3. Le théorème de Skolem-Noether fournit une représentation fidèle

$$\rho : \mathrm{Gal}(L/K) \to \mathrm{PGL}_n(D)$$

4. Ceci implique que D est un sous-corps propre de $\mathbb{Q}(\zeta_p)$ et $[D : \mathbb{Q}]n = p - 1$. En utilisant la théorie de CM, on trouve que D est à CM.

Démonstration esquissée

Démonstration esquissée

1. D'abord on montre que $\mathrm{End}^0(A) \cong M_n(D)$ où D est une algèbre à division de dimension finie sur $\mathbb{Q}$ qui satisfait $[D : \mathbb{Q}]n \leq 2g = p - 1$ et $n > 1$.
2. On observe que l'action de $\mathrm{Gal}(L/K)$ sur $M_n(D)$ par automorphismes est fidèle.
3. Le théorème de Skolem-Noether fournit une représentation fidèle

$$\rho : \mathrm{Gal}(L/K) \to \mathrm{PGL}_n(D)$$

4. Ceci implique que D est un sous-corps propre de $\mathbb{Q}(\zeta_p)$ et $[D : \mathbb{Q}]n = p - 1$. En utilisant la théorie de CM, on trouve que D est à CM.

Variétés abéliennes définies sur $\mathbb{Q}$

Théorème (G.'21)

Soit $A/\mathbb{Q}$ une variété abélienne de dimension $g \geq 1$ où $p = 2g+1$ est un nombre premier. Supposons $\mathrm{Gal}(\mathbb{Q}(A[2])/\mathbb{Q}) \cong C_p$. Alors

- *soit $\mathrm{End}^0(A)$ est un sous-corps propre de $\mathbb{Q}(\zeta_p)$;*
- *soit $p \equiv 3 \mod 4$ et $\mathrm{End}^0(A) \cong M_g(\mathbb{Q}(\sqrt{-p}))$.*

En particulier, il y a un nombre fini des possibilités pour $\mathrm{End}^0(A)$.

Ci-dessus et un résultat technique donnent :

Corollaire (G.'21)

Soit $C : y^2 = f(x)$ une courbe elliptique définie sur un corps avec un plongement réel. Si $\mathrm{Gal}(f) \cong C_3$, alors $\mathrm{End}(C) = \mathbb{Z}$.

Corollaire (G.'21)

Soit $A/\mathbb{Q}$ une surface abélienne. Supposons que $\mathrm{Gal}(\mathbb{Q}(A[2])/\mathbb{Q}) \cong C_5$. Alors soit $\mathrm{End}(A) = \mathbb{Z}$ soit $\mathrm{End}^0_{\mathbb{Q}}(A) = \mathrm{End}^0(A) = \mathbb{Q}(\sqrt{5})$.

Variétés abéliennes définies sur $\mathbb{Q}$

Théorème (G.'21)

Soit $A/\mathbb{Q}$ une variété abélienne de dimension $g \geq 1$ où $p = 2g+1$ est un nombre premier. Supposons $\mathrm{Gal}(\mathbb{Q}(A[2])/\mathbb{Q}) \cong C_p$. Alors

- *soit $\mathrm{End}^0(A)$ est un sous-corps propre de $\mathbb{Q}(\zeta_p)$;*
- *soit $p \equiv 3 \mod 4$ et $\mathrm{End}^0(A) \cong M_g(\mathbb{Q}(\sqrt{-p}))$.*

En particulier, il y a un nombre fini des possibilités pour $\mathrm{End}^0(A)$.

Ci-dessus et un résultat technique donnent :

Corollaire (G.'21)

Soit $C\colon y^2 = f(x)$ une courbe elliptique définie sur un corps avec un plongement réel. Si $\mathrm{Gal}(f) \cong C_3$, alors $\mathrm{End}(C) = \mathbb{Z}$.

Corollaire (G.'21)

Soit $A/\mathbb{Q}$ une surface abélienne. Supposons que $\mathrm{Gal}(\mathbb{Q}(A[2])/\mathbb{Q}) \cong C_5$. Alors soit $\mathrm{End}(A) = \mathbb{Z}$ soit $\mathrm{End}^0_{\mathbb{Q}}(A) = \mathrm{End}^0(A) = \mathbb{Q}(\sqrt{5})$.

Des pubs vont arriver

Vous aimeriez peut-être aussi...

Chabauty symétrique généralisé

Question (Zureick-Brown)

Est-il possible de déterminer les points cubiques sur $X_0(65)$, malgré le fait qu'il y a un infini de points quadratiques ?

Théorème (Box, Gajović, G. '21)

Soit $N \in \{53, 57, 61, 65, 67, 73\}$. Alors les points cubiques sur $X_0(N)$ sont connus. De plus, les points quartiques isolés sur $X_0(65)$ sont connus.

Pour démontrer ci-dessus, on prolonge les méthodes de "Chabauty symétrique" de Siksek et on a implémenté nos méthodes dans `Magma`.

Théorème (Box '21)

Des courbes elliptiques sur des corps quartiques complètement réels qui ne contiennent pas $\sqrt{5}$ sont modulaire.

Théorème (Banwait, Derickx)

Supposons GRH. Alors pour chaque nombre premier p :

$$Y_0(p)(\mathbb{Q}(\zeta_7)^+) \neq \emptyset \iff Y_0(p)(\mathbb{Q}) \neq \emptyset.$$

Chabauty symétrique généralisé

Question (Zureick-Brown)

Est-il possible de déterminer les points cubiques sur $X_0(65)$, malgré le fait qu'il y a un infini de points quadratiques ?

Théorème (Box, Gajović, G. '21)

Soit $N \in \{53, 57, 61, 65, 67, 73\}$. Alors les points cubiques sur $X_0(N)$ sont connus. De plus, les points quartiques isolés sur $X_0(65)$ sont connus.

Pour démontrer ci-dessus, on prolonge les méthodes de "Chabauty symétrique" de Siksek et on a implémenté nos méthodes dans `Magma`.

Théorème (Box '21)

Des courbes elliptiques sur des corps quartiques complètement réels qui ne contiennent pas $\sqrt{5}$ sont modulaire.

Théorème (Banwait, Derickx)

Supposons GRH. Alors pour chaque nombre premier p :

$$Y_0(p)(\mathbb{Q}(\zeta_7)^+) \neq \emptyset \iff Y_0(p)(\mathbb{Q}) \neq \emptyset.$$

Chabauty symétrique généralisé

Question (Zureick-Brown)

Est-il possible de déterminer les points cubiques sur $X_0(65)$, malgré le fait qu'il y a un infini de points quadratiques ?

Théorème (Box, Gajović, G. '21)

Soit $N \in \{53, 57, 61, 65, 67, 73\}$. Alors les points cubiques sur $X_0(N)$ sont connus. De plus, les points quartiques isolés sur $X_0(65)$ sont connus.

Pour démontrer ci-dessus, on prolonge les méthodes de "Chabauty symétrique" de Siksek et on a implémenté nos méthodes dans `Magma`.

Théorème (Box '21)

Des courbes elliptiques sur des corps quartiques complètement réels qui ne contiennent pas $\sqrt{5}$ sont modulaire.

Théorème (Banwait, Derickx)

Supposons GRH. Alors pour chaque nombre premier p :

$$Y_0(p)(\mathbb{Q}(\zeta_7)^+) \neq \emptyset \iff Y_0(p)(\mathbb{Q}) \neq \emptyset.$$

Courbes superelliptiques avec des grosses images de Galois

Soient r un nombre premier, $f \in \mathbb{Q}(\zeta_r)[x]$ un polynôme sans facteur carrée.
Soit J la jacobienne de la courbe superelliptique définie par $y^r = f(x)$.

Théorème (G. '20)

Il y a des conditions de congruence sur f qui garantissent que les représentations

$$\rho_\ell \colon G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}(J[\ell])$$

ont des images aussi grosses que possible pour tout nombre premier ℓ hors d'un ensemble fini.

Par contre, ces images ont des formes bizarres, plutôt inattendues !

Images explicites

Théorème (G.'20)

Pour $r = 3$ et presque tout premier ℓ, l'image de

$$\rho_\ell \colon G_{\mathbb{Q}(\zeta_3)} \to \mathrm{Aut}(J[\ell])$$

est pour i impair :

$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_g(\ell)^{\lceil \frac{g}{3} \rceil, 6} \rtimes \langle \chi_\ell \rangle$$

et pour i pair :

$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GU}_g(\ell)^{\lceil \frac{g}{3} \rceil, 6}.\langle \chi_\ell \rangle.$$

Théorème (G.'20)

Soit $\ell \equiv 1 \mod r$. Alors pour tout premier ℓ hors d'un ensemble fini et explicite, on a :

$$\bar{\rho}_\lambda(G_{\mathbb{Q}(\zeta_r)}) = \mathrm{GL}_n(\ell)$$

où $n = \frac{2g}{r-1}$.

Quelques exemples

Pour $d \in \{12, 18, 24\}$ les courbes

$$y^3 - \zeta_3^2 \pi y^2 - \zeta_3^2 y = x^d + x^{d-1} + 7x^3 + 14x^2 + 45\zeta_3 \pi$$

où $\pi = 1 - \zeta_3$, ont une image aussi grosse que possible tout premier ℓ hors d'un ensemble fini et explicite.
En particulier, hors de cet ensemble, elles satisfont

$$\bar{\rho}_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_{d-2}(\ell) \text{ for } \ell \equiv 1 \mod 3\,;$$

et

$$\bar{\rho}_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \Delta\mathrm{U}_{d-2}(\ell) \text{ for } \ell \equiv 5, 29 \mod 36.$$

Quand $d = 12, 24$ le résultat ci-dessus reste vrai pour $\ell \equiv 5 \mod 12$.

Et une autre

Pour $\ell \neq 2, 3, 7, 41, 701, 1039501386253916593179$, ou
$43925848740498753191116327084384430459193646639059731257968697588808662051073513549304709161942299997692676257925754003306241063325843729755594846954361363671187723617963506593669934438819533140385381012723675 83$ la courbe superelliptique

$$y^7 = x^{14} + \pi x^{13} + 2\pi^7 x^7 + 6\pi^{12} x^2 + 246\pi^7$$

où $\pi = 1 - \zeta_7$, a une image maximale en ℓ.
Si $\lambda | \ell$ avec $\ell \equiv 1 \mod 7$, on a

$$\bar{\rho}_\lambda(G_{\mathbb{Q}(\zeta_7)}) = \mathrm{GL}_{12}(\ell)$$

et pour $\ell \equiv 13 \mod 28$

$$\bar{\rho}_\lambda(G_{\mathbb{Q}(\zeta_7)}) = \Delta\mathrm{U}_{12}(\ell).$$