Courbes superelliptiques avec des images grosses de Galois

Pip Goodman

Représentations mod ℓ

Soient ℓ un nombre premier, et A une variété abélienne principalement polarisée de dimension g sur un corps de nombres K.

Le groupe de ℓ-torsion de $A(\overline{K})$, c'est-à-dire, $A[\ell] := \{P \in A(\overline{K}) | \ell P = 0\}$ est un espace vectoriel de dimension $2g$ sur $\mathbb{F}_\ell$:

$$A[\ell] \cong \mathbb{F}_\ell^{2g}.$$

Le groupe de Galois absolu G_K agit linéairement sur cet espace, ce qui fournit une représentation

$$\rho_\ell \colon G_K \to \mathrm{GL}_{2g}(\ell).$$

De plus, l'accouplement de Weil (qui est un accouplement symplectique non-dégénéré) $A[\ell] \times A[\ell] \to \mathbb{F}_\ell^*$, est préservé à similitude près par G_K.

Cela force l'image de la représentation de prend ses valeurs dans le sous-groupe

$$\rho_\ell \colon G_K \to \mathrm{GSp}_{2g}(\ell).$$

Les images des mod ℓ représentations

Théorème de l'image ouvert de Serre
Soit E/K une courbe elliptique telle que $\mathrm{End}(E) \cong \mathbb{Z}$. Alors, pour presque tout nombre premier ℓ, on a $\mathrm{Gal}(K(E[\ell])/K) = \mathrm{GL}_2(\ell)$.

Théorème (Hall '08)
Soit $C : y^2 = f(x)$, où $f \in K[x]$ est sans facteur carré et de degré $2g+1$. Soit $J = \mathrm{Jac}(C)$. Supposons que $\mathrm{End}(J) \cong \mathbb{Z}$, et f ait une facteur carré modulo un nombre premier p. Alors, pour presque tout nombre premier ℓ, on a $\mathrm{Gal}(K(J[\ell])/K) = \mathrm{GSp}_{2g}(\ell)$.

Théorème (Anni, V. Dokchitser '20)
Soit g un entier postif tel que $2g+2$ satisfait "double Goldbach + ε". Alors, il est possible de trouver une courbe hyperelliptique définie sur $\mathbb{Q}$ de genre g telle que les représentions mod ℓ ont une image aussi grosse que possible, pour tout nombre premier ℓ.

Et pour les sous-groupes “naturels” de $\mathrm{GSp}_{2g}(\ell)$?

On s’attendrait à ce que l’image de ρ_ℓ soit aussi grosse que possible. C’est-à-dire, elle devrait être $\mathrm{GSp}_{2g}(\ell)$ sauf s’il y a une bonne raison.

Quelle est une bonne raison? Des endomorphismes!

Source naturelle des endomorphismes?

Soient r un nombre premier impair, $f \in \mathbb{Q}(\zeta_r)[x]$ sans facteur carré.

Soit C la courbe lisse et projective définie par

$$y^r = f(x).$$

Il y a un automorphisme naturel de C provenant de $y \mapsto \zeta_r y$.

Cela introduit automorphisme

$$[\zeta_r] \colon J \to J$$

sur la jacobienne J de C.

$[\zeta_r]$ fournit un automorphisme sur $J[\ell]$ pour chaque $\ell \neq r$.

Cet automorphisme préserve l'accouplement de Weil.

Donc la représentation

$$G_{\mathbb{Q}(\zeta_r)} \to \mathrm{GSp}_{2g}(\ell)$$

prend ses valeurs dans le centraliseur de $[\zeta_r] \in \mathrm{GSp}_{2g}(\ell)$.

Quelle est la forme du centraliseur de $[\zeta_r]$?

Comment faire pour montrer l'image de $\rho_\ell(G_K)$ est "aussi grosse que possible"?

Check-list de théorie des groupes

Théorème (Arias-de-Reyna, Dieulefait, Wiese '16)
Soit $G \leq \mathrm{GSp}_{2g}(\ell)$ un sous-groupe qui contient une transvection, où $\ell \geq 5$ est un nombre premier. Si G ne contient pas $\mathrm{Sp}_{2g}(\ell)$, alors une des suivantes est vérifiée:

- G est un sous-groupe réductible;
- G est un sous-groupe imprimitif.

Théorème (G.'20)
Soit $G \leq \mathrm{GL}_n(\ell^i)$ un sous-groupe qui contient une transvection, où $\ell \geq 5$ est un nombre premier. Si G ne contient pas $\mathrm{SL}_n(\ell^i)$, alors une des suivantes est vérifiée:

- G est un sous-groupe réductible;
- G est un sous-groupe imprimitif.
- G est contenu dans $\mathrm{GL}_n(\ell^j)$ où $j < i$;
- G est contenu dans $\mathrm{GSp}_n(\ell^i)$ ou $\mathrm{GU}_n(\ell^{i/2})$.

Irréductibilité and primitivité

Contrôle des sous-groupes d'inertie

Soit $\mathfrak{p}$ un idéal premier de $\mathbb{Q}(\zeta_r)$ au-dessus de p.

Théorème (T. Dokchitser '18)
Soit C une courbe définie par $f(x, y) = 0$ avec $f \in \mathbb{Q}(\zeta_r)[x, y]$, et f satisfait d'autres conditions.

Alors l'action du groupe d'inertie $I_{\mathfrak{p}}$ sur $V_\ell(\mathrm{Jac}(C))$, $p \neq \ell$, est déterminée par les valuations $\mathfrak{p}$-adiques des coefficients de f.

De plus, les résultats de Tim fournissent un modèle régulier de la courbe avec strict normal crossings. On s'en sert pour produire les transvections.

Jusqu'ici…

Théorème (G.'20)
Soit $d \geq 12$ un entier qui est divisible par $2r$ et est la somme de deux nombres premiers distincts $q_1 < q_2$.

Supposons qu'ils existent des nombres premiers $q_2 < q_3 < d$. Si $r > 23$ supposons que le nombre des classes de $\mathbb{Q}(\zeta_r)$ soit impair et $d = q_3 + 1$.

Alors étant donné un polynôme $f \in \mathbb{Q}(\zeta_r)[x]$ de degré d tel que ses coefficients satisfont certaines congruences, l'image de la représentation $\rho_\ell \colon G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}(J[\ell])$ contient les produits

- $\mathrm{SL}_n(\ell^i)^{\frac{r-1}{2i}}$ si le degré d'inertie i de ℓ dans $\mathbb{Q}(\zeta_r)$ est impair; et
- $\mathrm{SU}_n(\ell^{i/2})^{\frac{r-1}{i}}$ si le degré d'inertie i de ℓ dans $\mathbb{Q}(\zeta_r)$ est pair

pour tout ℓ hors d'un ensemble petit, fini et explicite.

Le dernier effort

J'ai regardé $y^3 = f(x)$ de genre g, et les premiers $p \equiv 1 \mod 3$, j'ai trouvé:

g	3	4	6	7
$\det \circ \rho_\lambda \left(\mathrm{Frob}_\mathfrak{p}\right)$	$p\mathfrak{p}$	$p\mathfrak{p}^2$	$p^2\mathfrak{p}^2$	$p^2\mathfrak{p}^3$

Théorie des multiplications complexes

Soit A/K une variété abélienne de dimension g telle que $\mathrm{End}^0(A)$ est un corps de nombres de dimension $2g$ sur $\mathbb{Q}$. On dit que A a des multiplications complexes.

L'algèbre des endomorphismes nous permet de regarder les représentations λ-adiques comme si elles étaient de dimension un, i.e., comme des caractères.

Le théorème principale des multiplication complexes nous informe qu'il existe un caractère algébrique de Hecke $\Omega\colon \mathbb{A}_K^* \to \mathbb{C}$ et chacun des représentations λ-adiques s'obtient à partir de Ω.

De plus, le type d'infini de Ω est déterminé par la formule de Shimura-Taniyama.

Dans notre cas, on obtient un caractère algébrique de Hecke qui donne lieu aux $\det \circ \rho_\lambda$.

Théorème (Fité ’20)
Soit A/K une variété abélienne avec $E = \mathrm{End}_K(A) \otimes \mathbb{Q}$ un corps de nombres. Supposons que $K \supseteq E$ et $E/\mathbb{Q}$ soient galoisiennes. Alors il existe une caractère algébrique d’Hecke $\Omega \colon \mathbb{A}_E^* \to \mathbb{C}$ dont les avatars λ-adique coïncident avec $\det \circ \rho_\lambda$ pour

$$\rho_\lambda \colon G_K \to \mathrm{Aut}(T_\lambda(A))$$

et le type d’infini est déterminé par l’action de $\mathrm{End}(A)$ sur $\Omega^0(A)$.

Maintenant on peut construire des courbes $y^r = f(x) \in \mathbb{Q}(\zeta_r)[x]$ de genre g dont la jacobienne J satisfait les théorèmes suivants:

Théorème (G.'20)
Pour 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 $\ell \neq 2, 3, 7, 41, 701, 10395013862539165931 79$, ou $4392584874049875319111632708438443045919364663905973125796869758880866205107351354930470916194229999769267625792575400330624106332584372975559484695436136367118772361796350659366993443881953314038538101272367583$ 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 $\ell \equiv 13 \mod 28$

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