Galois representations of elliptic curves and abelian entanglements

Brau Avila, Julio

Resume

Cette thèse étudie principalement les représentations galoisiennes attachées aux points de torsion des courbes elliptiques. Dans le premier chapitre, nous considérons le problème de déterminer l'image de la représentation ρ_E attachée à une courbe elliptique E définie sur $\mathbb{Q}$, sans multiplication complexe. Nous donnons un algorithme déterministe qui calcule l'image de ρ_E comme sous-groupe de $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, dont la sortie est un entier m et un sous-groupe fini $G(m) \subset \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. L'image de ρ_E est le sous-groupe des éléments de $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ dont la réduction modulo m appartient à $G(m)$.

Dans une seconde partie, nous développons une méthode utilisant des sommes de caractères, qui exploite l'image de ρ_E pour décrire les densités d'ensembles de premiers p pour lesquels la courbe réduite $\tilde{E}(\mathbb{F}_p)$ a certaines propriétés. Si E est une courbe elliptique définie sur $\mathbb{Q}$, il suit des travaux de Serre et Hooley que, sous l'Hypothèse de Riemann Généralisée, la densité des premiers p tels que le groupe des points $\mathbb{F}_p$-rationnels de la courbe réduite $\tilde{E}(\mathbb{F}_p)$ est cyclique s'écrit comme un produit infini $\prod \delta_\ell$ de facteurs locaux δ_ℓ liés au degré du corps contenant la ℓ-torsion, multiplié par un facteur correctif prenant en compte l'intrication de ces différents corps. Nous montrons que ce facteur correctif s'interprète comme somme de caractères et cette description nous permet de déterminer facilement s'il s'annule ou non. Nous appliquons notre méthode à d'autres situations, par exemple en restreignant p à une progression arithmétique fixée. Nous étudions

aussi les constantes apparaissant dans la conjecture de Koblitz, liée à la densité des p pour lesquels le groupe des $\mathbb{F}_p$-points de E est un nombre premier. Dans toutes ces applications, le thème unificateur sous-jacent est que les densités étudiées sont entièrement déterminées par l'image de ρ_E.

Une courbe elliptique sur $\mathbb{Q}$ est une *courbe de Serre* si l'image de la représentation galoisienne associée est aussi grande que possible, et la plupart des courbes elliptiques définies sur $\mathbb{Q}$ sont de ce type. Notre dernier chapitre se préoccupe de la classification des courbes qui ne sont pas courbes de Serre : nous exhibons une courbe modulaire de niveau 6 qui complète la liste des courbes modulaires paramétrant ces courbes. Cette courbe modulaire définit aussi une famille infinie de courbes elliptiques dont les «corps d'intrication» sont non abéliens. Les questions en suspens après le chapitre précédent, sur la classification des courbes elliptiques auxquelles nous pouvons appliquer la méthode des sommes de caractères, fournissent une motivation supplémentaire pour cette famille.