HOMOTHÉTIES DANS L'IMAGE DE GALOIS

Agnès David

***Résumé.* —** On présente dans cet exposé des résultats uniformes sur le sous-groupe des homothéties contenu dans l'image de la représentation galoisienne associée aux points de torsion d'une courbe elliptique.

Dans le cas où l'image de la représentation est triangulaire supérieure, on obtient des résultats supplémentaires décrivant les deux seules formes possibles pour sa diagonale.

1. Acteurs

1.1. Groupe de Galois. — On fixe K un sous-corps de $\mathbb{C}$ qui est de dimension finie comme espace vectoriel sur $\mathbb{Q}$ (un tel corps est appelé un corps de nombres). On s'intéresse au groupe, noté G_K, des automorphismes de corps de la clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ qui valent l'identité sur K. La théorie de Galois relie en effet l'étude de ce groupe à la compréhension des équations polynomiales à coefficients dans K.

1.2. Courbe elliptique. — On fixe également une courbe elliptique E définie sur le corps K ; une telle courbe est donnée par une équation polynomiale à coefficients dans K, à deux variables et de degré 3, à laquelle on adjoint un point à l'infini.

L'ensemble $E(\overline{\mathbb{Q}})$ des solutions de cette équation dans $\overline{\mathbb{Q}}$ (point à l'infini compris) est muni d'une structure de groupe abélien. Pour tout entier n plus grand que 1, l'ensemble des points de n-torsion de ce groupe est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^2$; si n est un nombre premier, cet ensemble forme en particulier un espace vectoriel de dimension 2 sur le corps à n éléments.

1.3. Une représentation galoisienne. — On fixe enfin p un nombre premier. Le groupe G_K agit sur $E(\overline{\mathbb{Q}})$, en respectant sa structure de groupe ; il agit donc également sur ses points de p-torsion. On en déduit une représentation φ_p de G_K, à valeurs (après choix d'une base pour les points de p-torsion) dans $GL_2(\mathbb{F}_p)$.

2. Un problème de Serre uniforme

2.1. Image de Galois. — On s'intéresse ici au sous-groupe de $GL_2(\mathbb{F}_p)$ qui est l'image de G_K par le morphisme de groupes φ_p. Cette image permet en effet de comprendre l'extension de K engendrée dans $\overline{\mathbb{Q}}$ par les coordonnées des points de p-torsion de E.

2.2. Un théorème de Serre. — Cette image est asymptotiquement grosse, au sens par exemple du théorème suivant.

***Théorème 2.1* (Serre [8]).** — *Si la courbe elliptique E n'a pas de multiplication complexe, alors il existe une borne $C(K,E)$, ne dépendant que du corps K et de E, vérifiant : si p est plus grand que $C(K,E)$, alors la représentation φ_p est surjective.*

L'interprétation de ce résultat est que l'extension de K engendrée par les coordonnées des points de p-torsion de E est aussi grosse que possible.

L'hypothèse initiale de l'énoncé porte sur l'anneau des endomorphismes de la courbe E : on sait qu'il est soit réduit à $\mathbb{Z}$, soit un sous-anneau d'indice fini de l'anneau des entiers d'un corps quadratique (extension de dimension 2 de $\mathbb{Q}$) imaginaire (n'admettant pas de plongement dans $\mathbb{R}$) ; selon le cas, on dit que E n'a pas ou a des multiplications complexes.

Dans le cas où la courbe possède des multiplications complexes, la représentation φ_p est précisément décrite ; son image contient un sous-groupe commutatif d'indice au plus 2 et ne peut donc pas être tout $GL_2(\mathbb{F}_p)$; en revanche, il existe des résultats selon lesquels elle est aussi asymptotiquement grosse, en un sens à adapter.

2.3. Une version uniforme ?— Dans [8], Serre suggère également qu'on peut s'affranchir de la dépendance en la courbe elliptique E dans la borne $C(K,E)$, pour obtenir une version uniforme du théorème 2.1. Un tel résultat n'est même pas encore connu lorsque le corps de base est $\mathbb{Q}$, malgré des résultats partiels importants de Mazur [3], Merel [4] et Parent [6].

3. Homothéties contenues dans l'image de Galois

Les matrices des homothéties constituent le centre de $GL_2(\mathbb{F}_p)$. Pour montrer que l'image de la représentation φ_p est uniformément grosse, il est donc naturel de chercher à montrer qu'elle contient uniformément un gros sous-groupe des homothéties.

Nous avons obtenu le résultat uniforme suivant :

***Théorème 3.1* (David [1], Eckstein[2]).** — *Il existe une borne $C(K)$, explicite et ne dépendant que du corps de nombres K, telle que si p est plus grand que $C(K)$, alors l'image de φ_p contient toutes les puissances douzièmes des homothéties.*

Notre démonstration donne une forme explicite pour la borne $C(K)$, qui la fait dépendre de nombreux invariants arithmétiques du corps de nombres K (degré, discriminant, nombre de classes, régulateur, etc.).

Remarque 3.2. — Le théorème 3.1 ne fournit pas toutes les homothéties comme sous-groupe de l'image de la représentation φ_p, mais seulement leurs puissances douzièmes. Cette puissance douzième apparaît naturellement dans le cours de la démonstration pour trivialiser les images de certains sous-groupes qui dépendent de la courbe elliptique, mais dont l'ordre est borné. D'autre part, Eckstein présente dans sa thèse **[2]** un exemple pour lequel l'image de φ_p ne contient pas toutes les homothéties ; il s'agit d'un exemple où la courbe elliptique possède des multiplications complexes. On peut donc se demander si, en ajoutant l'hypothèse que la courbe E n'a pas de multiplication complexe, il est possible de montrer que l'image de φ_p contient toutes les homothéties.

4. Éléments de démonstration

4.1. Image de l'inertie et sous-groupes maximaux. — La démonstration du théorème 3.1 repose sur le dialogue entre deux idées.

La première est que les homothéties recherchées se trouvent dans l'image de certains sous-groupes de G_K, appelés les sous-groupes d'inertie associés à p. La restriction de la représentation φ_p à ces sous-groupes est bien connue, grâce à des travaux de Serre **[8]** et Raynaud **[7]**.

La seconde est la connaissance des sous-groupes maximaux de $GL_2(\mathbb{F}_p)$ qui peuvent contenir l'image de φ_p si celle-ci n'est pas tout $GL_2(\mathbb{F}_p)$. On peut déjà choisir, uniformément, p assez grand pour que ces sous-groupes maximaux soient de deux types : normalisateur d'un sous-groupe de Cartan (cas traité par Eckstein) ou sous-groupe de Borel (conjugué aux matrices triangulaires supérieures).

4.2. Cas d'une représentation triangulaire supérieure. — On suppose désormais que l'image de la représentation φ_p est incluse dans un sous-groupe de Borel (c'est-à-dire, dans une base qui lui est adaptée, triangulaire supérieure). La recherche des homothéties qu'elle contient passe alors par des résultats précis sur la forme que peut prendre la représentation.

4.2.1. Caractères. — La représentation φ_p étant triangulaire supérieure, sa diagonale est donnée par deux morphismes de groupes de G_K dans $\mathbb{F}_p^\times$, appelés des caractères de G_K. Chacun de ces deux caractères diagonaux est plus facile à étudier que la représentation entière, notamment car son image est commutative (et même cyclique). La théorie du corps de classes fournit en effet des outils puissants pour l'étude de l'extension de K, finie et de groupe de Galois abélien, qui lui est associée.

4.2.2. Deux formes pour la diagonale. — En utilisant et explicitant des travaux de Momose **[5]**, on montre qu'il n'y a que deux possibilités pour la puissance douzième de la diagonale de φ_p, lorsque p est plus grand que la borne $C(K)$:

– soit elle est formée de deux caractères égaux ;

– soit elle présente de grandes similarités avec celle associée à une courbe elliptique ayant des multiplications complexes.

Dans les deux cas, on peut en déduire que les puissances douzièmes des homothéties sont contenues dans l'image de la représentation.

4.2.3. Lien avec le problème de Serre uniforme. — Lorsque le corps de base est $\mathbb{Q}$, Mazur **[3]** a montré que l'ensemble des nombres premiers p pour lesquels l'image de φ_p peut être contenue dans un sous-groupe de Borel est fini (et borné par 163). Au vu de la liste des sous-groupes maximaux de $GL_2(\mathbb{F}_p)$ donnée en 4.1, ce résultat constitue une partie importante du théorème de Serre uniforme sur $\mathbb{Q}$. Sa généralisation à un corps de nombres K quelconque consisterait à montrer que, pour chacun des deux types de diagonale précédemment obtenus, soit p est plus petit qu'une borne ne dépendant que de K, soit la courbe E possède effectivement des multiplications complexes.

4.2.4. Méthode de démonstration. — La démonstration du résultat sur la diagonale de φ_p débute par une étude fine de la situation locale aux places hors de p et de l'action des sous-groupes d'inertie au-dessus de p.

On applique ensuite à une place hors de p la loi de réciprocité donnée par la théorie du corps de classes globale ; on obtient ainsi des relations entre toutes les informations locales, sous forme de congruences modulo p. Pour p assez grand, ces congruences deviennent des égalités, liant fortement les situations locales hors et au-dessus de p.

Une version effective du théorème de Chebotarev permet enfin de se ramener à un nombre fini de places hors de p pour obtenir une borne ne dépendant que de K et reconstruire les caractères diagonaux.

On obtient en réalité trois types possibles pour la puissance douzième de la diagonale de φ_p ; l'un d'eux, pour lequel l'un des deux termes diagonaux est trivial, est éliminé en utilisant les bornes uniformes sur l'ordre des points de torsion (**[4]**, **[6]**).

Références

[1] A. David, *Caractère d'isogénie et borne uniforme pour les homothéties*, Thèse de doctorat, Université Louis Pasteur (Strasbourg), 2008.

[2] C. Eckstein, *Homothéties, à chercher dans l'action de Galois sur des points de torsion*, Thèse de doctorat, Université Louis Pasteur (Strasbourg), 2005.

[3] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), *Invent. Math.*, t. 44(2), 1978, p. 129-162.

[4] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, *Invent. Math.*, t. 124(1-3), 1996, p. 437-449.

[5] F. Momose, Isogenies of prime degree over number fields, *Compositio Math.*, t. 97(3), 1995, p. 329-348.

[6] P. Parent, Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres, *J. Reine Angew. Math.*, t. 506, 1999, p. 85-116.

[7] M. Raynaud, Schémas en groupes de type $(p, \dots, p)$, *Bull. Soc. Math. France*, t. 102, 1974, p. 241-280.

[8] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.*, t. 15(4), 1972, p. 259-331.

Agnès David

UMPA - ÉNS Lyon, 46 allée d'Italie, 69364 Lyon Cedex 07.

E-mail : `Agnes.David@ens-lyon.org`