Introduction au domaine de recherche : courbes elliptiques et q-nombres de Weil.

Thomas Agugliaro

Table des matières

1 Introduction **1**

2 Courbes elliptiques **1**
2.1 Le strict minimum sur les courbes elliptiques 1
2.2 Courbes elliptiques sur les corps finis 3

3 q-nombre de Weil et théorie de Honda-Tate **4**
3.1 q-nombres de Weil 4
3.2 La classification 6

4 Applications : comprendre les variétés abéliennes à travers le Frobenius **8**

1 Introduction

Si q est la puissance d'un nombre premier p, les q-nombres de Weil sont des entiers algébriques reliés à des objets de géométrie algébrique sur le corps $\mathbb{F}_q$, par exemple aux courbes elliptiques. La motivation de l'étude de ces nombres est donc surtout tournée vers la géométrie algébrique, mais il n'y a aucun prérequis nécessaire pour suivre mon IDR.

2 Courbes elliptiques

2.1 Le strict minimum sur les courbes elliptiques

Soient k un corps de caractéristique différente de 2 ou 3, et $\overline{k}$ une clôture algébrique de k.

Remarque 2.1. *On peut aussi étudier les courbes elliptiques sur des corps de caractéristique* 2 *ou* 3*, mais dans ce cas les définitions qui suivent ne seraient pas correctes.*

Définition 2.2. *Une courbe elliptique sur k est un sous-ensemble E de $\overline{k}^2$ de la forme*

$$\{(x,y) \in \overline{k}^2 | \quad y^2 = x^3 + ax + b\}$$

pour des éléments a et b de k tels que $\Delta = -16(4a^3 + 27b^3)$ soit non nul.

Remarque 2.3. *Ces objets sont aussi munis d'une stucture de groupe, c'est-à-dire qu'étant donné une courbe elliptique E, on a une loi de composition interne*

$$\begin{aligned} m : E \times E &\to E \\ (x,y),(x',y') &\mapsto (P(x,y,x',y'), Q(x,y,x',y')) \end{aligned}$$

faisant de E un groupe abélien, où P et Q sont des fractions rationnelles à quatre variables à coefficients dans k.
En réalité, cette définition manque de rigueur, il faut rajouter un point 0_E, "à l'infini" à E pour avoir une telle loi de groupe, et ce point sera l'élément neutre. Ce point à l'infini sert à donner une valeur aux pôles de P et Q. De plus, cette loi de groupe est uniquement déterminée par E, on peut aussi en donner une construction plus géométrique.

Définition 2.4. *Soient E et F deux courbes elliptiques. Un morphisme de courbes elliptiques est une application $f : E \to F$ de la forme*

$$(x,y) \mapsto (P(x,y), Q(x,y))$$

où P et Q sont des fractions rationnelles à deux variables à coefficients dans k. L'ensemble des morphismes de E vers F sera noté $\mathrm{Hom}_k(E,F)$.

Remarque 2.5. *Un tel morphisme est automatiquement un morphisme de groupes !*

Définition 2.6. *Soient E et F deux courbes elliptiques, on dira que E et F sont isogènes s'il existe un morphisme non constant*

$$f : E \to F.$$

Un tel morphisme sera appelé une isogénie.

On va maintenant voir des exemples d'isogénies : si n est un entier naturel et E une courbe elliptique, on définit

$$\begin{aligned} [n]_E : E &\to E \\ x &\mapsto x +_E x +_E \cdots +_E x \end{aligned}$$

où il y a n fois l'élément x dans la somme. On peut vérifier que $[n]_E$ est un morphisme, il faut vérifier que l'application est polynomiale au niveau des coordonnées de x. Et c'est bien le cas car $+_E$ est définie par des polynômes. Il est plus délicat de prouver $[n]_E$ est non constante, c'est pour ça que je vais l'admettre pour la suite. On peut aussi définir $[n]_E$ pour un entier négatif.
Ces isogénies que je viens de définir ont un statut particulier, d'après la proposition suivante.

Proposition 2.7. *Soient E et F deux variétés abéliennes et $f : E \to F$ une isogénie. Alors il existe une isogénie $g : F \to E$ et un entier naturel n tels que*

$$f \circ g = [n]_F, \quad g \circ f = [n]_E.$$

Il y a un résultat important de finitude sur les Hom entre courbes elliptiques.

Proposition 2.8. *Soient E et F deux courbes elliptiques. Alors le groupe $\mathrm{Hom}_k(A, B)$ est un $\mathbb{Z}$-module libre de rang fini.*

Le fait qu'il soit sans torsion découle du fait que les $[n]_E$ sont des isogénies, le fait qu'il soit de type fini est un résultat plus profond.

Définition 2.9. *Soient E et F deux courbes elliptiques, on définit le $\mathbb{Q}$-espace vectoriel de dimension finie $\mathrm{Hom}_k^0(E, F) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}_k(E, F)$. De même, on a une $\mathbb{Q}$-algèbre (non nécessairement commutative) de dimension finie $\mathrm{End}_k^0(A) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_k(A)$.*

Remarque 2.10. *La proposition 2.8 prouve que $\mathrm{End}_k^0(A)$ est un corps non commutatif. En effet, toute isogénie de A dans A qui est non nulle admet un inverse quitte à diviser par un entier naturel n.*

2.2 Courbes elliptiques sur les corps finis

On supposera dorénavant que k est un corps fini de caractéristique p différente de 2 et 3 (même si cela est superflu en général), de cardinal q et on fixera $\overline{k}$ une clôture algébrique de k.
Tout ce qui a été fait à la section précédente s'applique encore, et il y a des nouveautés qui apparaissent sur un corps fini.

Définition 2.11. *Soit E une courbe elliptique définie sur k, donnée par l'équation*

$$y^2 = x^3 + ax + b$$

avec a et b dans k. Alors l'application

$$\begin{aligned} \pi_E : E &\to E \\ (x, y) &\mapsto (x^q, y^q) \end{aligned}$$

est appelée le Frobenius de E.

Remarque 2.12. *Si E est une courbe elliptique sur k, π_E est à priori définie sur E à valeurs dans $\overline{k}^2$. Mais on peut vérifier que la subtilité de la caractéristique p fait que π_E est bien à valeur dans E. Soit $(x, y) \in E$, alors*

$$(y^q)^2 = (y^2)^q = (x^3 + ax + b)^q = x^{3q} + a^q x^q + b^q.$$

Et comme $a, b \in k$ on a $a^q = a$ et $b^q = b$. D'où

$$(y^q)^2 = (x^q)^3 + ax^q + b$$

et on a bien $(x^q, y^q) \in E$.

Remarque 2.13. *Si l est une extension finie de k, alors c'est aussi un corps fini, soit q^n son cardinal. Une courbe elliptique E sur k peut aussi être vue sur l car $\overline{k}$ est une clôture algébrique de l et on peut interpréter les coefficients a et $b \in k$ définissant E comme des éléments de l. Mais alors le Frobenius de E vu comme une courbe elliptique sur l n'est pas le même que lorsqu'elle est vue comme une courbe elliptique sur k. En fait on a $\pi_{E,l} = \pi_{E,k}^n$ avec des notations évidentes car pour $(x, y) \in E$:*

— $\pi_{E,k}(x, y) = (x^q, y^q)$
— $\pi_{E,l}(x, y) = (x^{q^n}, y^{q^n}) = \pi_{E,k}^n(x, y)$.

Ainsi, sur les corps finis, les courbes elliptiques ont des endomorphismes privilégiés $\pi_E \in \mathrm{End}_k(E)$. On peut alors considérer le corps de nombres engendré par π_E dans $\mathrm{End}_k^0(E)$, que l'on notera $\mathbb{Q}(\pi_E)$. On peut alors considérer π_E comme un entier algébrique dans un corps de nombres, et c'est le point de départ de la classification des courbes elliptiques à isogénie près par la théorie de Honda-Tate.

Théorème 2.14 (Hasse)**.** *Soit E une courbe elliptique sur le corps fini k. Pour tout plongement complexe $\sigma : \mathbb{Q}(\pi_E) \hookrightarrow \mathbb{C}$, on a*

$$|\sigma(\pi_E)| = \sqrt{q}.$$

Remarque 2.15. *Ici $|z|$ désigne le module d'un nombre complexe z.*

Un tel entier algébrique s'appelera un q-nombre de Weil. C'est l'objet de la section suivante.

3 q-nombre de Weil et théorie de Honda-Tate

3.1 q-nombres de Weil

Soit q une puissance d'un nombre premier. On fixera $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ et on considérera le sous-ensemble $\overline{\mathbb{Z}}$ de $\overline{\mathbb{Q}}$ constitué des *entiers algébriques.*

Définition 3.1. *Un q-nombre de Weil est un élément $\alpha \in \overline{\mathbb{Z}}$ tel que pour tout plongement $\sigma : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ on ait $|\sigma(\alpha)| = \sqrt{q}$.*

Proposition 3.2. *Soit α un q-nombre de Weil, alors il existe un unique q-nombre de Weil noté $\overline{\alpha}$ tel que pour tout plongement $\sigma : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ on ait*

$$\sigma(\overline{\alpha}) = \overline{\sigma(\alpha)}.$$

De plus, $\overline{\alpha} = \frac{q}{\alpha}$. Ici $\overline{\sigma(\alpha)}$ désigne le conjugué complexe de $\sigma(\alpha) \in \mathbb{C}$.

Démonstration. L'unicité provient de l'injectivité de n'importe quel plongement complexe. Pour l'existence, on pose $\overline{\alpha} = \frac{q}{\alpha}$, alors si σ est un plongement complexe on a

$$\sigma(\overline{\alpha}) = \frac{q}{\sigma(\alpha)} = \frac{\sigma(\alpha)\overline{\sigma(\alpha)}}{\sigma(\alpha)} = \overline{\sigma(\alpha)}.$$

$\overline{\alpha}$ est bien un entier algébrique, car si P est un polynôme unitaire à coefficients dans $\mathbb{Z}$ annulé par α alors il est aussi annulé par $\overline{\alpha}$ (on applique la conjugaison complexe à la relation $P(\alpha) = 0$). □

De plus, on peut construire des q-nombres de Weil explicitement sans référence aux variétés sur les corps finis.
Soit α un q-nombre de Weil, on lui associe $\beta = \alpha + \overline{\alpha}$. Alors β est un entier algébrique tel que pour tout plongement complexe σ, on ait $\sigma(\beta) \in \mathbb{R}$ et $|\sigma(\beta)| \leqslant 2\sqrt{q}$. On a donc défini une application

$$R : \{q - \text{nombres de Weil}\} \to \{\beta \in \overline{\mathbb{Z}} \,|\forall \sigma : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}, \sigma(\beta) \in \mathbb{R}, |\sigma(\beta)| \leqslant 2\sqrt{q}\}.$$

Proposition 3.3. *Cette application est surjective, passe au quotient par la conjugaison, et induit une bijection entre les classes de conjugaisons de q-nombres de Weil et les classes de conjugaisons d'éléments du codomaine de R.*

Démonstration. Soit $\beta \in \overline{\mathbb{Q}}$ dans le codomaine de R. Le trinôme

$$X^2 - \beta X + q$$

a pour discriminant $\Delta = \beta^2 - 4q$. Soient α_1 et α_2 ses racines, ce sont des entiers algébriques. Ainsi pour tout plongement $\sigma : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$

$$\sigma(\Delta) = \sigma(\beta)^2 - 4q \leqslant (2\sqrt{q})^2 - 4q = 0.$$

Alors pour tout plongement σ, on a que $\sigma(\alpha_1)$ et $\sigma(\alpha_2)$ sont conjugués complexes l'un de l'autre. Par relation coefficients-racines on a que $\alpha_1\alpha_2 = q$, donc pour tout plongement σ, $\sigma(\alpha_1)\sigma(\alpha_2) = q$. Donc $\sigma(\alpha_1)$ est de module $\sqrt{q}$. Et par relations coefficients racines $\beta = \alpha_1 + \alpha_2$, donc α_1 est un q-nombre de Weil et $R(\alpha_1) = \beta$, d'où la surjectivité.
Si α est un q-nombre de Weil, et $w(\alpha)$ est un conjugué, où $w \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, alors

$$w(R(\alpha)) = w(\alpha) + w(\overline{\alpha}) = w(\alpha) + \overline{w(\alpha)} = R(w(\alpha)).$$

Donc R passe au quotient, et il reste à montrer que l'application induite est injective.
Soient α_1 et α_2 des q-nombres de Weil tels que $R(\alpha_1) = w(R(\alpha_2)$ avec $w \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Alors α_2 est racine du polynôme

$$P(X) = X^2 - R(\alpha_2)X + q,$$

et en appliquant w à l'égalité $P(\alpha_2) = 0$, on obtient que $w(\alpha_1)$ est racine du polynôme

$$Q(X) = X^2 - w(R(\alpha_2))X + q.$$

Et comme $w(R(\alpha_2)) = R(\alpha_1)$ on obtient que $w(\alpha_1) = \alpha_1$ ou $\overline{\alpha_1}$. □

La proposition précédente nous informe que pour construire des q-nombres de Weil, il suffit de construire des $\beta \in \overline{\mathbb{Z}}$ tels que pour tout plongement complexe σ on ait $\sigma(\beta) \in \mathbb{R}$ (un tel nombre sera appelé *totalement réel*), et $|\sigma(\beta)| \leqslant 2\sqrt{q}$ (un tel nombre sera appelé *totalement borné par* $2\sqrt{q}$).
Il est facile de construire des nombres totalement réels : il y en a des classiques comme $\phi = \frac{1+\sqrt{5}}{2}$ ou $\sqrt{2+\sqrt{2}}$, et plus généralement étant donné un polynôme de degré n à coefficients réels, on peut l'approcher par un polynôme irréductible de degré n à coefficients rationnels. On peut le voir comme une conséquence du théorème d'approximation faible, mais malheureusement cela produit des polynômes à coefficients rationnels dont on ne contrôle pas bien les dénominateurs. Ainsi, on peut construire des entiers algébriques totalement réels, mais on ne contrôle pas vraiment leurs tailles. Cependant on peut toujours choisir un q assez grand pour obtenir des q-nombres de Weil π et appliquer la théorie de Honda-Tate pour des corps finis assez gros.

3.2 La classification

Soit k un corps fini de cardinal q. Étant donné une courbe elliptique E sur k, elle a un endomorphisme privilégié $\pi_E \in \mathrm{End}_k(E)$ qui à un point de coordonnées (x, y) associe (x^q, y^q). On peut donc considérer $\pi_E \in \mathrm{End}_k^0(E)$, et $\mathrm{End}_k^0(E)$ est un corps d'après la remarque 2.10, et est de dimension finie sur $\mathbb{Q}$. Ainsi, π_E possède un polynôme minimal P_E sur $\mathbb{Q}$, et on peut interpréter π_E comme une racine de P_E, donc interpréter π_E comme un entier algébrique. C'est la classe de conjugaison de cet entier algébrique qui servira d'invariant classifiant la courbe elliptique E.

Soit W l'ensemble des q-nombres de Weil, et soit $\mathcal{W} = W/\sim$ où $\sim$ est la restriction à W de la relation de conjugaison sur $\overline{\mathbb{Q}}$ (autrement dit, deux q-nombres de Weil sont équivalents s'ils ont le même polynôme minimal sur $\mathbb{Q}$). Soit $\mathcal{I}$ l'ensemble des courbes elliptiques sur k à isogénies près.

Théorème 3.4 (Tate)**.** *La flèche qui a une courbe elliptique E sur k associe l'ensemble des racines de P_E dans $\overline{\mathbb{Q}}$ passe au quotient en une application $\mathcal{I} \to \mathcal{W}$ qui est injective.*

Remarque 3.5. *Le fait que les racines de P_E soient des q-nombres de Weil découle du théorème de Hasse 2.14. Le fait que la flèche passe au quotient découle du fait que $\mathrm{End}_k^0(A)$ est invariant par isogénies et que le Frobenius commute aux morphismes de variétés définies sur k. Pour voir ça, étant donné $f : E \to F$ ainsi que $g : F \to E$ telles que $f \circ g = [n]_F$ et $g \circ f = [n]_E$ pour un certain entier n, on définit un morphisme d'algèbres*

$$\begin{aligned} \mathrm{End}_k^0(E) &\to \mathrm{End}_k^0(F) \\ u &\mapsto \frac{1}{n} f \circ u \circ g. \end{aligned}$$

C'est clairement un isomorphisme de réciproque $u \mapsto \frac{1}{n} g \circ u \circ g$. Le Frobenius est dans le centre de $\mathrm{End}_k^0(E)$ car l'action du groupe de Galois commute aux

morphismes de variétés définis sur k. En conséquence, le morphisme précédent associe à π_E l'endomorphisme de F suivant :

$$\frac{1}{n} f \circ \pi_A \circ g = \frac{1}{n} f \circ g \circ \pi_B$$

car g est défini sur k. Or $\frac{1}{n} f \circ g = \mathrm{id}_F$ par définition de f et g, donc le Frobenius de E est envoyé sur le Frobenius de F par l'isomorphisme défini précédemment. Donc le polynôme minimal de π_E est le même que le polynôme minimal de π_F, et donc l'application définie dans 3.4 passe bien au quotient.

L'étape suivante est de comprendre l'image de l'application $\mathcal{I} \to \mathcal{W}$. Il va donc falloir trouver des conditions supplémentaires sur les Frobenius des courbes elliptiques, la proposition suivante nous donne des conditions dont la nature se trouve en théorie algébrique des nombres.

Proposition 3.6 (Tate)**.** *Soit E une courbe elliptique, $F = \mathbb{Q}(\pi_E)$ le corps de nombres associé. Si pour toute place $v|p$ on pose*

$$a_v = \frac{v(\pi)}{v(q)} [F_v : \mathbb{Q}_p] \in \mathbb{Q}$$

où F_v est le complété de F pour la place v, et soit m le plus petit commun multiple des dénominateurs des a_v (sous forme irréductible). Alors

$$m \deg_{\mathbb{Q}} \pi_E = 2.$$

Ainsi on peut considérer $W_1 \subset W$ le sous-ensemble formé des éléments π de W satisfaisant aux conditions du théorème précédent. C'est-à-dire les π tels que si m est le ppcm des

$$\frac{v(\pi)}{v(q)} [F_v; \mathbb{Q}_p]$$

pour $v|p$, on a $m \deg_{\mathbb{Q}} \pi = 2$.
Le sous-ensemble W_1 est stable par conjugaison, donc on peut considérer le quotient $\mathcal{W}_1 \subset \mathcal{W}$. Le théorème suivant nous dit que ce sous-ensemble de $\mathcal{W}$ est l'image de l'application définie dans le théorème 3.4.

Théorème 3.7 (Honda)**.** *Soit $\pi \in \mathcal{W}_1$, alors il existe une courbe elliptique E sur k telle que π soit conjugué à l'entier algébrique $\pi_E \in \mathbb{Q}(\pi_E) \subset \overline{\mathbb{Q}}$.*

Ainsi, on interpréte des objets provenant de la géométrie algébrique sur les corps finis en utilisant des outils de théorie algébrique des nombres.

Remarque 3.8. *Le théorème de Honda est en fait plus général, je l'ai énoncé pour les courbes elliptiques pour en simplifier la présentation.*

On a une application injective $\mathcal{I} \to \mathcal{W}$ dont l'image est $\mathcal{W}_1$. On peut donc se demander si les éléments de $\mathcal{W} \setminus \mathcal{W}_1$ correspondent aussi à des objets de la géométrie algébrique sur k. C'est le cas, il existe une généralisation des courbes

elliptiques appelées les variétés abéliennes, c'est-à-dire que les courbes elliptiques sont les variétés abéliennes de dimension 1. Et toute la théorie des courbes elliptiques que j'ai exposée a un sens pour les variétés abéliennes, mais la théorie des variétés abéliennes requiert plus de technicité, pour une référence il y a [Mum70]. On peut aussi considérer $\mathcal{I}_{\text{ab}}$ l'ensemble des variétés abéliennes *simples* à isogénies près.

Théorème 3.9 (Honda-Tate)**.** *Il y a une application $\mathcal{I}_{\text{ab}} \to \mathcal{W}$ qui étend l'application définie dans le théorème 3.4. Cette application est une bijection.*

Remarque 3.10. *L'injectivité est dûe à Tate en 1966 dans son article [Tat66] et la surjectivité est due à Honda en 1968, qui est exposée par exemple dans [Tat71].*

4 Applications : comprendre les variétés abéliennes à travers le Frobenius

Cette section sera plus difficile, je vais commencer cette section par un commentaire qu'il n'est pas nécessaire de comprendre.

Remarque 4.1. *Soit k un corps fini, la théorie de Honda-Tate associe à chaque variété abélienne A un entier algébrique π. Et certaines questions de géométrie algébrique sur A se traduisent en termes du Frobenius π. Par exemple, il est possible de comprendre l'algèbre d'endomorphismes $\text{End}_k^0(A)$ en termes de théorie algébrique des nombres et de π, à l'aide de la théorie de Brauer des corps de nombres.*
Une application récente est la démonstration par mon encadrant Giuseppe Ancona de la conjecture standard de type Hodge pour les variétés abéliennes de dimension 4 [Anc20]. Il utilise (entre autres) la théorie de Honda-Tate. Sa preuve contient plusieurs étapes, la partie que je vais regarder ici est la preuve que certaines représentations Galoisiennes sont de dimension 2.
Soient A une variété abélienne simple de dimension 4, et π son Frobenius. Les représentations qui nous intéressent proviennent de puissances extérieures d'une représentation ayant comme "valeurs propres"

$$\pi_1, \dots, \pi_8$$

qui sont les conjugués de π. Ainsi les puissances extérieures auront des "valeurs propres"

$$\prod_{i \in I} \pi_i$$

pour I un sous-ensemble de $\{1, \dots, 8\}$.
On s'intéresse à la sous-représentation qui est l'espace propre pour q^2. Ainsi, on s'intéresse aux sous-ensembles I de $\{1, \dots, 8\}$ tels que $\prod_{i \in I} \pi_i = q^2$. Comme $|\pi_i| = \sqrt{q}$ on a $|I| = 4$. Plus particulièrement, on étudie le cas où I contient soit π_i soit π_{i+g} pour $i \in \{1, \dots, g\}$ mais pas les deux. En effet la relation

$\pi_1\overline{\pi_1}\pi_2\overline{\pi_2} = q^2$ *convient, mais elle n'est pas remarquable, dans le sens où elle ne dépend pas de* π*. L'étude de ces relations est une propriété purement de théorie des nombres, ainsi c'est un exemple d'incarnation de la théorie de Honda-Tate.*

Soit π un q-nombre de Weil, dont on numérote $\pi_1, \pi_2, \dots, \pi_{2g}$ les conjugués de telle sorte que $\overline{\pi_i} = \pi_{i+g}$. La conclusion de la remarque précédente est que : c'est une question intéressante d'étudier les relations de la forme $\prod_{i\in I} \pi_i = q^a$ où I est un sous-ensemble de $\{1, \cdots, 2g\}$ de cardinal pair $2a$. Giuseppe Ancona traite le cas où il y a 8 conjugués, il y a d'autres cas qui sont traités de la même manière (en se basant sur [Anc20]) dans l'article de Koshikawa [Kos22]. Dans le cas où g est impair, quitte à étendre les scalaires, π devient π^2, et alors une relation $\prod_{i\in I} \pi_i = q^{g/2}$ peut se réécrire $\prod_{i\in I} \frac{q}{\pi_i^2} = 1$. On peut alors introduire les quantités

$$\beta_i = \frac{q}{\pi_i^2}.$$

La question d'étudier les relations entre les π_i devient alors une question d'étude de relations entre les β_i pour $i \in \{1, \dots, g\}$. On peut considérer $\mathcal{F}$ le groupe abélien libre à g générateurs $\beta_1, \dots, \beta_g$. Alors le noyau du morphisme de groupe universel $\mathcal{F} \to \mathbb{Q}(\beta_1, \dots, \beta_{2g})^\times$ est "l'ensemble des relations entre les β_i", ainsi si ce noyau est libre de rang 1 cela donne des informations sur les produits qui nous intéressent.
Or le noyau de ce morphisme est de rang 1 si et seulement si l'image est de rang $g-1$ et c'est la condition sous laquelle Koshikawa travaille dans son article. Il détermine ainsi ce noyau : soit $\beta_1^{a_1} \dots \beta_g^{a_g}$ un générateur du noyau avec $a_i \in \mathbb{Z}$. Le groupe de Galois de $\mathbb{Q}(\beta_1, \dots, \beta_{2g})/\mathbb{Q}$ agit transitivement sur les racines, et il préserve le noyau. Donc il agit à travers $\{1, -1\}$ sur le noyau. Ainsi, pour tout i, $a_i = \pm a_1$. Donc quitte à renuméroter les π_i en inversant π_i avec π_{i+g} pour certains i, un générateur de "l'ensemble des relations" est $(\beta_1 \dots \beta_g)^N$.
Cette information sur l'ensemble des relations entre les β_i permet d'obtenir des informations cruciales sur les variétés abéliennes qu'il étudie.

Références

[Anc20] Giuseppe Ancona. Standard conjectures for abelian fourfolds. *Inventiones mathematicae*, 223(1) :149–212, aug 2020.

[Kos22] Teruhisa Koshikawa. The numerical hodge standard conjecture for the square of a simple abelian variety of prime dimension, 2022.

[Mum70] David Mumford. *Abelian varieties.* Published for the Tata Institute of Fundamental Research, 1970.

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones Mathematicae*, 2(2) :134–144, 1966.

[Tat71] John Tate. Classes d'isogénie des variétés abéliennes sur un corps fini. In *Séminaire Bourbaki : vol. 1968/69, exposés 347-363*, number 11 in Séminaire Bourbaki. Springer-Verlag, 1971. talk :352.