POINTS RATIONNELS ET UNIFORMITÉ

NOTES PRISES PAR ZIYANG GAO

Troisième partie 3. Résultat sur la conjecture de torsion par Cadoret–Tamagawa

1. Module de Tate l-adique des variétés abéliennes

(10/02/2021 par Marc Hindry)

1.1. **Groupe fondamental.** Commençons par une discussion générale. Soit X un espace topologique connexe et localement connexe par arcs. Le *groupe de Poincaré* de X est défini par $\pi_1^{\mathrm{top}}(x_0, X) = \{\text{lacets}\}/\{\text{homotopie}\}$. Ce group classifie les revêtements (topologiques localement) de X. En effet, soit $X^{\mathrm{univ}} \to X$ le revêtement universel, alors $\mathrm{Aut}(X^{\mathrm{univ}}/X) = \pi_1^{\mathrm{top}}(x_0, X)$. Pour tout revêtement $\pi \colon Y \to X$, il existe une application $X^{\mathrm{univ}} \to Y$ telle que le diagramme commute

$$\begin{tikzcd} X^{\mathrm{univ}} \arrow[r] \arrow[d] & Y \arrow[dl, "\pi"] \\ X & \end{tikzcd}$$

Remarquons que $X^{\mathrm{univ}} \to Y$ est un revêtement de Y. Notons $H = \mathrm{Aut}(X^{\mathrm{univ}}/Y)$. Alors H est un sous-groupe de $\pi_1^{\mathrm{top}}(x_0, X)$. De plus, cette discussion est liée à la théorie de Galois par le lemme suivant.

Lemme 1.1. *Le revêtement $Y \to X$ est galoisien (c'est-à-dire* $\mathrm{Aut}(Y/X)$ *agit transitivement sur les fibres) si et seulement si $H \lhd \pi_1^{\mathrm{top}}(x_0, X)$. Si ceci est vrai, alors* $\mathrm{Aut}(Y/X) = \pi_1^{\mathrm{top}}(x_0, X)/H$.

Maintenant l'on regarde les variétés algébriques. Soit X une variété algébrique irréductible définie sur un corps K.

Si $K = \mathbb{C}$, alors $X(\mathbb{C})$ est un espace topologique connexe et localement connexe par arcs, et l'on ainsi le groupe de Poincaré $G := \pi_1^{\mathrm{top}}(X(\mathbb{C}))$ défini comme dessus. De plus, l'on a $H_1(X(\mathbb{C}), \mathbb{Z}) = G^{\mathrm{ab}}$.

Pourtant, le revêtement universel $X^{\mathrm{univ}} \to X$ n'est en général pas algébrique. Pour rester dans la catégorie algébrique, l'on considère seulement les revêtements finis $f \colon Y \to X$, qui correspondent aux sous-groupes H de G d'indice fini. Pour ces revêtements, Y est encore une variété algébrique et f est un morphisme algébrique. Ceci inspire la définition suivante du groupe fondamental algébrique.

Définition 1.2. $\pi_1^{\mathrm{alg}}(X) = \varprojlim_{H \lhd G \text{ d'indice fini}} G/H$.

Autrement dit, $\pi_1^{\mathrm{alg}}(X)$ classifie les revêtements finis (algébriques) de X.

Exemple 1.3. *Si* $G = \mathbb{Z} = \pi_1^{\mathrm{top}}(\mathbb{G}_m(\mathbb{C}))$, *alors le revêtement universel est* $\exp\colon \mathbb{C} \to \mathbb{C}^*$. *Dans ce cas-là, l'on a* $\pi_1^{\mathrm{alg}}(\mathbb{G}_m) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}} = \prod \mathbb{Z}_p$.

En général, $\pi_1^{\mathrm{top}}(X(\mathbb{C}))$ est un groupe discret de type fini, mais $\pi_1^{\mathrm{alg}}(X)$ est un groupe profini muni de la topologie où les sous-groupes distingués finis forment un système fondamental de voisinages de l'élément neutre.

Si K est un sous-corps de $\mathbb{C}$, l'on a de plus une action de $\Gamma_K := \mathrm{Gal}(\overline{K}/K)$ sur les groupes π_1, H_1, *etc.*

1.2. **Variétés abéliennes et modules de Tate.** Soit A une variété abélienne sur un corps K.

Nous voulons voir ce que c'est $\pi_1^{\mathrm{alg}}(A)$, pour K quelconque.

Commençons par le cas $K = \mathbb{C}$. Dans ce cas-là, $A(\mathbb{C}) = \mathbb{C}^g/\Omega$ pour un réseau $\Omega \simeq \mathbb{Z}^{2g}$ dans $\mathbb{C}^g$. De plus, il y a la forme de Riemann qui donne une polarisation sur A (telle que A est une variété projective). Il est facile de voir que $\pi_1^{\mathrm{top}}(A(\mathbb{C})) = \Omega$ et donc $H_1(A(\mathbb{C}), \mathbb{Z}) = \Omega$. L'on a

$$\begin{aligned}\pi_1^{\mathrm{alg}}(A) &= \varprojlim(\Omega/n\Omega)\\ &= \varprojlim \left(\frac{1}{n}\Omega/\Omega\right)\\ &= \varprojlim \mathrm{Ker}\left([n]\colon A(\mathbb{C}) \to A(\mathbb{C})\right).\end{aligned}$$

Ceci suggère la définition de π_1^{alg} pour A/K avec K un corps quelconque.

Maintenant K est un corps arbitraire. Posons

$$A[n] := \mathrm{Ker}\left([n]\colon A(\overline{K}) \to A(\overline{K})\right),$$

et

$$\widehat{T}(A) := \varprojlim_n A[n]. \tag{1.1}$$

Définition 1.4. *Soit l un nombre premier. Le module de Tate l-adique de A est défini comme*

$$T_l(A) := \varprojlim_n A[l^n].$$

Remarque 1.5. *Pour ceux qui connaissent la cohomologie étale, l'on a en effet* $H_1^{\text{ét}}(A_{\overline{K}}, \mathbb{Z}_l) = T_l(A)$ *(autrement dit, un revêtement fini étale d'une variété abélienne est encore une variété abélienne). Donc* $H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Z}_l) = \mathrm{Hom}(T_l(A), \mathbb{Z}_l)$.

Lemme 1.6 (Weil)**.** *Soit* $p = \mathrm{car}(K)$. *Alors*

$$A[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{2g} \qquad \text{si } p \nmid n, \tag{1.2}$$

et

$$A[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^{r_p(A)} \tag{1.3}$$

avec $r_p(A) \in \{0, \ldots, g\}$ *qui ne dépend pas de* n.

Par conséquent, si $l \neq \mathrm{car}(K)$, alors $T_l(A) \simeq \mathbb{Z}_l^{2g}$ en tant que $\mathbb{Z}_l$-modules. Dans la suite, nous supposons toujours $l \neq \mathrm{car}(K)$.

Le groupe de Galois $\Gamma_K = \mathrm{Gal}(\overline{K}/K)$ agit sur $T_l(A)$ comme suit. L'action $\Gamma_K \times A(\overline{K}) \to A(\overline{K})$ induit naturellement une action $\Gamma_K \times A[n] \to A[n]$, d'où l'action de Γ_K sur $T_l(A)$ qui est continue. L'on obtient ainsi une représentation continue l-adique galoisienne [1]

$$\rho_l \colon \Gamma_K \to \mathrm{GL}(T_l(A)) \simeq \mathrm{GL}_{2g}(\mathbb{Z}_l). \tag{1.4}$$

L'image du morphisme ρ_l est un sous-groupe compact, donc fermé, de $\mathrm{GL}_{2g}(\mathbb{Z}_l)$. Donc $\rho_l(\Gamma_K)$ est un groupe de Lie l-adique.

Théorème 1.7. *Soit $\phi \colon A \to B$ un morphisme entre deux variétés abéliennes définies K. Alors ϕ induit un morphism $T_l(\phi) \colon T_l(A) \to T_l(B)$, et l'on obtient ainsi un morphisme*

$$\mathrm{Hom}(A,B) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{Hom}_{\mathbb{Z}_l[\Gamma_K]}(T_l(A), T_l(B)).$$

Ce morphisme est

(i) injectif;

(ii) un isomorphisme si K est de type fini sur $\mathbb{Q}$ ou $\mathbb{F}_p$.

La deuxième partie de ce théorème est *la conjecture de Tate* pour les variétés abéliennes. Elle a été démontrée par Faltings lorsque K est un corps de nombres, par Tate lorsque $K = \mathbb{F}_p$ et par Zarhin lorsque K est de type fini sur $\mathbb{F}_p$.

Lorsque la deuxième partie du Théorème 1.7 est vraie, l'on a

$$V_l(A) \simeq_{\Gamma_K} V_l(B) \Leftrightarrow A \sim_K B \ (K\text{-isogénie}). \tag{1.5}$$

Théorème 1.8 (Critère de Néron–Ogg–Shafarevich)**.** *Si K est un corps de nombre et soit v une place finie de K. Alors A a bonne réduction en v si et seulement si $T_l(A)$ est non-ramifié pour un $l \neq p_v$.*

En pratique, il est plus simple de considérer l'enveloppe algébrique $G_{l,K}$ de $\rho_l(\Gamma_K)$ définie comme suit.

Définition 1.9. *Le $\mathbb{Q}_l$-groupe algébrique $G_{l,K}$ est défini comme l'adhérence de Zariski de $\rho_l(\Gamma_K)$ dans $\mathrm{GL}_{2g}(\mathbb{Q}_l)$.*

Voici un lemme facile.

Lemme 1.10. *Pour toute extension finie K'/K, l'on a*

$$G_{l,K}^\circ = G_{l,K'}^\circ.$$

Grâce à ce lemme, le $\mathbb{Q}_l$-groupe algébrique $G_l := G_{l,K}^\circ$ est bien défini. Quitte à remplacer K par une extension finie, l'on a $\rho_l(\Gamma_K) \subseteq G_l(\mathbb{Z}_l)$.

Théorème 1.11 (Bogomolov, (Serre, Tate))**.** *Supposons que K est un corps de type fini sur $\mathbb{Q}$. Alors*

$$\rho_l(\Gamma_K) \subseteq G_l(\mathbb{Q}_l)$$

est une inclusion ouverte.

[1]. Pour chaque n, ρ_l induit $\rho_{A,l^n} \colon \Gamma_K \to \mathrm{GL}_{2g}(\mathbb{Z}/l^n\mathbb{Z})$ via $A[l^n] = T_l(A)/l^n T_l(A)$. Si $\mathrm{car}(K) = 0$, l'on a de plus $\widehat{\rho} \colon \Gamma_K \to \mathrm{GL}(\widehat{T}(A)) \simeq \mathrm{GL}_{2g}(\widehat{\mathbb{Z}})$.

Une variante de ce théorème est : $\rho_l(\Gamma_K) \subseteq G_l(\mathbb{Z}_l)$ est d'indice fini.

Remarque 1.12. *Ce théorème reste vrai pour d'autres variétés que les variétés abéliennes. Il se repose sur la semisimplicité, qui est connue pour par exemple les variétés abéliennes.*

Lorsque K est un corps de nombres, le Lemme 1.10 peut être renforcé.

Proposition 1.13. *Supposons que K est un corps de type fini sur $\mathbb{Q}$. Alors il existe une extension finie K^{conn} de K telle que $G_{l,K^{\mathrm{conn}}} = G_l^\circ$ pour tout l.*

1.3. **La conjecture de Mumford–Tate.** Dans cette sous-section, supposons que K est un corps de type fini sur $\mathbb{Q}$. Remplaçons K par K^{conn}. Alors $G_l = G_l^\circ$ pour tout l.

Nous voudrons

(i) décrire le sous-$\mathbb{Q}_l$-groupe algébrique G_l de GL_{2g} ;

(ii) estimer l'indice $c_l := [G_l(\mathbb{Z}_l) : \rho_l(\Gamma_K)]$.

Pour les courbes elliptiques, l'on a le *théorème d'image ouverte* de Serre.

Théorème 1.14 (Serre '71)**.** *Soit E une courbe elliptique définie sur K sans CM sur $\overline{K}$. Alors pour tout l, $\rho_l(\Gamma_K) \subseteq \mathrm{GL}_2(\mathbb{Z}_l)$ est d'indice fini. De plus, il existe un nombre $l_0 = l_0(E, K)$ tel que*

$$\rho_l(\Gamma_K) = \mathrm{GL}_2(\mathbb{Z}_l) \quad \text{pour tout } l \geq l_0. \tag{1.6}$$

Une conséquence de (1.6) est que $\widehat{\rho}_E \colon \Gamma_K \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ est d'image ouverte.

En général, l'on ne peut pas espérer avoir le même résultat. En effet, voici deux restrictions évidentes sur G_l : l'image de Galois doit respecter la polarisation (l'accouplement de Weil) et les endomorphismes.

$\boxed{\text{Polarisation}}$ Soit

$$e_{\mathrm{Weil}} \colon A[n] \times A^\vee[n] \to \mu_n = \mathbb{G}_m[n]$$

l'accouplement de Weil, qui est bi-additif et non-dégénéré. Soit

$$\lambda \colon A \to A^\vee$$

la polarisation. Alors l'accouplement

$$e_\lambda \colon A[n] \times A[n] \to \mu_n, \quad (x, y) \mapsto e_{\mathrm{Weil}}(x, \lambda(y))$$

est anti-symétrique. Il est non-dégénéré si $(n, \deg \lambda) = 1$. Maintenant, e_λ induit un accouplement Γ_K-equivariant

$$E_\lambda \colon T_l(A) \times T_l(A) \to T_l(\mathbb{G}_m) = \mathbb{Z}_l(1).$$

Ceci donne un sous-groupe $\mathrm{GSp}_{2g,\lambda}$ de GL_{2g}, qui contient G_l.

$\boxed{\text{Endomorphismes}}$ Chaque élément $\alpha \in \mathrm{End}_{\overline{K}}(A)$ induit un élément de $\mathrm{End}(T_l(A))$ qui commute avec $\rho(\Gamma_K)$ et donc G_l.

Posons $D := \mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$. Alors ceci donne un sous-groupe $\mathrm{GSp}_{2g,\lambda}(D)$ de $\mathrm{GSp}_{2g,\lambda}$, qui contient G_l.

Théorème 1.15 (Deligne)**.** *Posons MT_A le groupe de Mumford–Tate de A. Alors l'on a $\mathrm{MT}_A \otimes \mathbb{Q}_l \subseteq \mathrm{GSp}_{2g,\lambda}(D)$ et*

$$G_l \subseteq \mathrm{MT}_A \otimes \mathbb{Q}_l. \tag{1.7}$$

La clé pour démontrer (1.7) est le résultat suivant de Deligne : tout cycle de Hodge d'une variété abélienne est un cycle de Hodge absolu.

Ce théorème répond à la question (i) de cette sous-section.

La question (ii), estimation de c_l, est la conjecture de Mumford–Tate.

Conjecture 1.16 (Conjecture de Mumford–Tate). *L'inclusion* (1.7) *est une égalité, c'est-à-dire* $G_l \subseteq \mathrm{MT}_A \otimes \mathbb{Q}_l$..

Nous terminons cette sous-section par la comparaison entre (G_l, ρ_l) et $(\mathrm{MT}_A, \rho_{\mathrm{MT}})$.

	$(\mathrm{MT}_A, \rho_{\mathrm{MT}})$	(G_l, ρ_l)
	groupe réductif	groupe réductif (Faltings '83)
centre	$Z(\mathrm{MT}_A)$	$Z(G_l) = Z(\mathrm{MT}_A) \otimes \mathbb{Q}_l$
facteurs du dérivé	de type A, B, C, D	pareil (Pink)
commutant dans $\mathrm{GSp}_{2g,\lambda}$	$\mathrm{End}^0(A)$	$\mathrm{End}^0(A) \otimes \mathbb{Q}_l$ (Faltings)
rang		$\mathrm{rg}(G_l)$ ne dépend pas de l

Par un théorème dans la théorie des groupes algébriques (les sous-groupes réductifs d'un groupe algébrique sont déterminés par le commutant et le rang), les deux dernières lignes de ce tableau impliquent : si la conjecture de Mumford–Tate est vraie est un nombre premier l, alors elle est vraie pour tout l.

1.4. **UOI de Cadoret–Tamagawa.** Soit K un corps de type fini sur $\mathbb{Q}$. Sauf indications contraires, π_1 est π_1^{alg} dans la suite.

Soit $f\colon X \to \mathrm{Spec}K$ géométriquement connexe. Alors f induit une suite exacte

$$0 \to \pi_1^{\mathrm{geom}}(X) := \pi_1(X_{\overline{K}}) \to \pi_1(X) \to \pi_1(\mathrm{Spec}K) = \Gamma_K \to 0.$$

Pareil, tout point rationnel $x \in X(K)$, qui est un morphisme $x\colon \mathrm{Spec}K \to X$, induit $\sigma_x\colon \Gamma_K \to \pi_1(X)$.

Si l'on a une représentation $\rho\colon \pi_1(X) \to \mathrm{GL}_m(\mathbb{Z}_l)$, alors tout $x \in X(K)$ induit

$$\rho_x = \rho \circ \sigma_x \colon \Gamma_K \to \mathrm{GL}_m(\mathbb{Z}_l). \tag{1.8}$$

Théorème 1.17 (C-T, 2012). *Soit $\mathcal{A} \to X$ un schéma abélien sur une courbe normale géométriquement irréductible définie sur K. Soit*

$$\rho\colon \pi_1(X) \to \mathrm{GL}_m(\mathbb{Z}_l) \tag{1.9}$$

une représentation l-adique satisfaisant

`(GLP)` : $\rho(\pi_1^{\mathrm{geom}}(X))^{\mathrm{ab}}$ *est fini et idem pour les sous-groupe ouverts.*

Alors l'on a

(i) l'ensemble exceptionnel

$$\mathcal{E}xp(\rho) := \{x \in X(K) : \rho_x(\Gamma_K) \text{ n'est pas ouverte dans } G := \rho(\pi_1(X))\}$$

est fini, où ρ_x est obtenue par (1.8).

(ii) si $x \in X(K) \setminus \mathcal{E}xp(\rho)$, alors $[G : \rho_x(\Gamma_K)] \leq B = B(\mathcal{A}/X, \rho)$.

Nous terminons cet exposé par l'application du théorème d'image ouverte uniforme, soit le Théorème 1.17, à la conjecture de torsion. Le résultat est une généralisation d'un résultat de Manin.

Maintenant, soit $\mathcal{A} \to X$ un schéma abélien sur une courbe normale géométriquement irréductible définie sur K. La fibre générique $\mathcal{A}_\eta$ est une variété abélienne sur $K(X)$. Donc l'on a une représentation continue l-adique galoisienne

$$\Gamma_{K(X)} \to \mathrm{GL}_{2g}(\mathbb{Z}_l). \tag{1.10}$$

D'autre part, le point générique $\eta\colon \mathrm{Spec}K(X) \to X$ donne $\Gamma_{K(X)} \to \pi_1(X)$.

Comme X est un schéma normal géométriquement irréductible, (1.10) est non-ramifiée car toutes les fibres sont lisses. Donc (1.10) se factorise par $\pi_1(X)$, d'où la représentation ρ désirée (celle de (1.9)).

Posons $\pi_n\colon \mathrm{GL}_{2g}(\mathbb{Z}_l) \to \mathrm{GL}_{2g}(\mathbb{Z}/l^n\mathbb{Z})$ pour tout n. Posons

$$G(n) := G \cap \mathrm{Ker}(\pi_n).$$

Théorème 1.17.(ii) implique alors que $G(n_0) \subseteq \rho_x(\Gamma_K)$ pour tout $x \in X(K) \setminus \mathcal{E}xp(\rho)$. Comme $\mathcal{E}xp(\rho)$ est un ensemble fini par Théorème 1.17.(i), nous avons démontré :

Corollaire 1.18. *Il existe un entier $N = N(\mathcal{A}/X, l)$ tel que $\mathcal{A}_x[l^\infty](K) \subseteq \mathcal{A}_x[l^N](K)$ pour tout $x \in X(K)$.*

1.5. **Cycles de Hodge vs. cycles de Hodge absolus.** Soit X une variété projective lisse définie sur un corps K.

Commençons par le cas où $K = \mathbb{C}$. Nous avons d'une part la structure sur $\mathbb{Q}$ de $H^i(X(\mathbb{C}), \mathbb{C})$ d'autre part la décomposition de Hodge :

$$H^i(X(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{C} = H^i(X(\mathbb{C}), \mathbb{C}) = \bigoplus_{p+q=i} H^{p,q}(X).$$

Il n'est pas difficile de voir

$$\{\text{cycles algébriques de codimension } i\} \subseteq H^{i,i}(X) \cap H^{2i}(X(\mathbb{C}), \mathbb{Q}).$$

La conjecture de Hodge prédit que cette inclusion est en effet une égalité.

Tout élément dans $H^{i,i}(X) \cap H^{2i}(X(\mathbb{C}), \mathbb{Q})$ s'appelle un *cycle de Hodge*.

Maintenant, si K peut se prolonger dans $\mathbb{C}$, alors pour chaque plongement $\sigma\colon K \hookrightarrow \mathbb{C}$ la discussion ci-dessus vaut pour $X_\sigma := X \otimes_{\sigma,K} \mathbb{C}$. Pourtant, les cycles de Hodge ainsi obtenus dépendent à priori du prolongement σ. Un *cycle de Hodge absolu* est un cycle de Hodge dont le conjugué par tout automorphisme de $\mathbb{C}$ reste un cycle de Hodge. Deligne a démontré, pour les variétés abéliennes, que tout cycle de Hodge est en effect Hodge absolu.