ANNALES DE L'INSTITUT FOURIER

PIERRE PARENT

Torsion des courbes elliptiques sur les corps cubiques

Annales de l'institut Fourier, tome 50, n° 3 (2000), p. 723-749

<http://www.numdam.org/item?id=AIF_2000__50_3_723_0>

Ann. Inst. Fourier, Grenoble
50, 3 (2000), 723–749

TORSION DES COURBES ELLIPTIQUES SUR LES CORPS CUBIQUES

par Pierre PARENT

Table des matières.

Mots-clés : Courbes elliptiques – Points rationnels – Symboles modulaires.
Classification math. : 11G05 – 14G05.

1. Présentation des résultats.

1.1. Introduction.

Soit E une courbe elliptique sur un corps de nombres K. Selon le théorème de Mordell-Weil, la partie de torsion $E(K)_{\text{tors}}$ du $\mathbb{Z}$-module $E(K)$ est de la forme $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, pour $n, m > 0$, n divisant m. Pour tout entier d, notons $\Phi(d)$ les classes d'isomorphismes des groupes finis G tel qu'il existe un corps de nombres K de degré d et E une courbe elliptique sur K vérifiant $E(K)_{\text{tors}} \simeq G$.

1.2. Théorème (Mazur, Kamienny, Abramovich, Merel). — *Pour tout d, $\Phi(d)$ est fini.*

(Voir [9], [19] ; on trouve dans [22] une version effective de ce théorème, plus précisément une borne pour l'ordre des éléments de $\Phi(d)$.) Pour tout d, notons $S(d)$ l'ensemble des nombres premiers p tel qu'il existe un élément de $\Phi(d)$ dont l'ordre est divisible par p. Pour justifier l'intérêt de $S(d)$, on peut noter qu'avant que Merel ne démontre la forme générale du théorème 1.2, Mazur et Kamienny avaient prouvé, à partir de travaux de Faltings et Frey, que ce résultat équivalait à ce que pour tout d, $S(d)$ soit fini ([9]). Pour d quelconque, on dispose maintenant pour les éléments de $S(d)$ d'une borne fournie par Oesterlé ([21]) :

$$\text{si } p \in S(d), \text{ alors } p \leq (1 + 3^{d/2})^2$$

(sauf peut-être pour $d = 3$ et $p = 43$).

Pour les petits degrés, on a des résultats plus précis :

1.3. Théorème (Mazur, Kamienny ; Kenku et Momose). — *Avec les notations précédentes,*

$$S(1) = \{2, 3, 5, 7\} \quad \textit{et} \quad S(2) = \{2, 3, 5, 7, 11, 13\}.$$

(On dispose même des listes $\Phi(1)$ et $\Phi(2)$.) Dans [9], Kamienny et Mazur conjecturent que les éléments de $S(3)$ sont inférieurs ou égaux à 19. Le but de cet article est de prouver qu'on a un peu mieux, sous réserve — pour $17 \leq p \leq 43$ — d'assertions $(*)_p$ suivantes (impliquées pour tout p par la conjecture de Birch et Swinnerton-Dyer) :

$(*)_p$ Le quotient d'enroulement de $J_1(p)$ est de rang nul sur $\mathbb{Q}$.

(Pour la définition du quotient d'enroulement et l'état des lieux à propos de $(*)_p$, voir les sections 1.5 et 2.1.)

1.4. THÉORÈME. — *Tout premier inférieur ou égal à* 13 *appartient à* $S(3)$. *Tout élément de* $S(3)$ *est inférieur ou égal à* 43. *Supposons l'assertion* $(*)_p$ *précédente vraie pour tout* p *premier,* $17 \leq p \leq 43$. *Alors si* p *appartient à* $S(3)$, $p \leq 17$. *Il n'existe qu'un nombre fini (inférieur ou égal à* 49) *de courbes elliptiques ayant de la* 17*-torsion sur un corps cubique, à isomorphisme près (ici on dit que deux courbes elliptiques sur deux corps* E/K *et* E'/K' *sont isomorphes s'il existe un isomorphisme de corps de* K' *dans* K, *et un isomorphisme de courbes elliptiques de* E *dans* $E' \times_{K'} K$).

À propos de la première assertion du théorème, notons que Zimmer *et al.* [23] donnent des familles de courbes sur des corps cubiques ayant de la 11-torsion, et d'autres de la 13-torsion. De plus, des travaux de Momose (voir [20]) montraient déjà (inconditionnellement) que 19 et 23 n'appartiennent pas à $S(3)$.

La démonstration, dont le plan va être présenté à la section suivante, reprend la méthode de Mazur avec la courbe modulaire X_1 à la place de X_0, et «en réduisant en 2». (La réduction en $\ell > 2$ donne au mieux la borne $(1 + \ell^{d/2})^2 > 37$, voir 1.5; la réduction en 2 pose en revanche des problèmes techniques nouveaux, voir 1.7 et la discussion qui lui fait suite. D'autre part, le genre de $X_0(p)$ pour les p considérés ici est inférieur à 3, ce qui montre que le «critère de Kamienny cubique» (voir 2.7 et 1.10) ne peut être satisfait avec X_0, et impose donc de travailler avec X_1.) Des calculs sur ordinateur ont été nécessaires. On a par ailleurs utilisé dans un premier temps les tables (non publiées) de [13], et les calculs de William Stein [29] disponibles par voie électronique; nos calculs avec machine sur l'homologie des courbes modulaires nous ont en fait permis de les retrouver indépendamment — au moins dans les cas que nous avons utilisés — en donnant les polynômes caractéristiques des opérateurs de Hecke.

Remarque. — Les calculs explicites faits sur l'algèbre de Hecke pour $J_1(19)$ en 4.2 montrent que celle-ci est engendrée, au moins sur $\mathbb{Z}[1/3]$, par les opérateurs losanges. D'autre part, le théorème 1.4 (sous l'hypothèse $(*)_{19}$), ou (inconditionnellement) les travaux de Momose [20] cités plus haut montrent que 19 n'appartient pas à $S(3)$. Cela infirme la «conjecture d'Ogg généralisée» faite par Kamienny (voir [9], [8]).

Remerciements. — Je tiens à remercier Loïc Merel qui a initié ce travail et m'a fait part de ses idées, Frédéric Lehobey pour ses conseils concernant la programmation, et bien sûr Bas Edixhoven qui a encadré le tout.

1.5. Structure de la démonstration : méthode de Mazur.

On va dans cette section exposer la méthode de Mazur sous une forme générale (pour X_1, en niveau premier, degré et «premier de réduction» quelconques), puis on explicitera en 1.11 son application aux corps cubiques.

Comme précédemment, donnons-nous une courbe elliptique E sur un corps de nombres K de dimension d sur $\mathbb{Q}$, et P un point de E à valeurs dans K, d'ordre un nombre premier p. Fixons un nombre premier ℓ différent de p. Notons $\mathcal{E}$ le modèle de Néron de E sur l'anneau $\mathcal{O}_K$ des entiers de K (on continue à noter P son prolongement à tout $\mathrm{Spec}(\mathcal{O}_K)$). Soit F le corps résiduel d'une place λ de $\mathcal{O}_K$ au-dessus de ℓ. Si $\mathcal{E}$ a bonne réduction en λ, alors on a (Hasse-Weil) :

$$\#\mathcal{E}(F) \leq \left(1 + (\#F)^{1/2}\right)^2.$$

Les multiples de P définissent un sous-schéma en groupes fermé de $\mathcal{E}$ qui est fini et plat de rang p sur $\mathcal{O}_K$, donc étale sur le lieu de la base où p est inversible, en particulier en toute place au-dessus de ℓ ; on en déduit $p \leq (1 + \ell^{d/2})^2$. Si $\mathcal{E}$ a réduction additive, alors $p \leq 3$; si $\mathcal{E}$ a réduction multiplicative non déployée, on a $p \leq (1 + \ell^d)$. Supposons qu'en toute place au-dessus de ℓ, $\mathcal{E}$ ait mauvaise réduction multiplicative déployée. Si la réduction de P est contenue dans la composante neutre de $\mathcal{E}_F$ en une place au-dessus de ℓ, on a $p \leq (\ell^d - 1)$. Supposons alors de plus qu'en toute place au-dessus de ℓ, la réduction de P soit d'image non triviale dans le groupe des composantes de $\mathcal{E}_F$.

On va noter $X_1(p)$ un modèle sur $\mathbb{Z}[1/p]$ de la surface de Riemann $X_1(p)(\mathbb{C})$, différent du modèle le plus usuel : pour nous, dans toute la suite, $X_1(p)$ sera l'objet paramétrant les couples (E, μ) où E est une courbe elliptique, et μ est une immersion fermée de schémas en groupes de μ_p dans E (voir [3], 8.2.2, et [5], prop. 2.1 ; le «modèle usuel» paramètre les immersions de $\mathbb{Z}/p\mathbb{Z}$ dans E).

Revenons au couple $(\mathcal{E}, P)$ considéré plus haut. Le point P permet de définir une immersion fermée α de schémas en groupes : $(\mathbb{Z}/p\mathbb{Z})_K \to \mathcal{E}_K$; on en déduit une immersion fermée de schémas en groupes, β : $(\mu_p)_K \to E' := \mathcal{E}_K/\mathrm{im}(\alpha)$ (β envoie $(\mu_p)_K$ sur le noyau de l'isogénie duale de $E \to E'$; voir [11], 2.8). Notons $\mathcal{E}'$ le modèle de Néron de E' sur $\mathcal{O}_K$. Le couple $(\mathcal{E}', \beta)$ donne un point j à valeurs dans $\mathcal{O}_K$ de $X_1(p)$, j se réduit en une pointe en chacune des places divisant ℓ, et chacune de ces pointes a pour image la pointe ∞_F dans $X_0(p)(F)$ (on choisit sur $\mathbb{Z}[1/p]$ un modèle quelconque pour $X_0(p)$). Soit $\sigma_1, \ldots, \sigma_d$ les plongements de K dans

une clôture algébrique de $\mathbb{Q}$; les $\sigma_i(j)$ se réduisent également, au-dessus de chaque place qui divise ℓ, en des pointes de $X_1(p)(F)$ d'image ∞_F dans $X_0(p)(F)$. Considérons la puissance symétrique d-ième de $X_1(p)$: le point $j^{(d)} := \sigma_1(j) + \cdots + \sigma_d(j)$ est dans $X_1(p)^{(d)}(\mathbb{Q})$. Par ailleurs chaque pointe $\sigma_i(j)_F$ se relève en une pointe $P_{0,i}$ de $X_1(p)$ à valeurs dans $\mathbb{Z}[1/p]$, s'interprétant modulairement comme un 1-gone (une copie de $\mathbb{P}^1$ qu'on a recollée le long des sections 0 et ∞), muni d'un μ_p; $P_{0,i}$ s'envoie sur ∞ dans $X_0(p)$. Le point $j^{(d)}$ a donc la même réduction en ℓ que la somme de d pointes $P_0 := P_{0,1} + \cdots + P_{0,d}$. (Notons que notre choix de modèle pour $X_1(p)$ est motivé uniquement par le fait qu'il permette d'obtenir à partir de notre courbe elliptique $\mathcal{E}$, par la construction ci-dessus, des pointes de $X_1(p)$ au-dessus de la pointe $\infty_{\mathbb{F}_\ell}$ de $X_0(p)$: cette convention est cruciale dans la suite, pour pouvoir utiliser la formule (3.5.12) de [28] citée à la fin de 2.6. En fait, on aurait aussi pu utiliser le « modèle usuel » pour $X_1(p)$, mais il aurait alors fallu faire une extension des scalaires à $\mathbb{Z}[1/p, \zeta_p]$ (ζ_p racine primitive p-ième de l'unité), et utiliser une « involution d'Atkin-Lehner » pour se ramener à des pointes au-dessus de ∞.)

Pour contrôler cette situation de mauvaise réduction multiplicative déployée, seul cas où on ne sait pas majorer p, on va se servir des considérations géométriques élémentaires suivantes.

MÉTHODE DE MAZUR. — *S'il existe une variété abélienne A sur $\mathbb{Q}$ (dont on note encore A le modèle de Néron sur $\mathbb{Z}_{(\ell)}$), et un morphisme $f_{P_0} : X_1(p)^{(d)} \to A$, normalisé par $f_{P_0}(P_0) = 0$ et vérifiant l'hypothèse :*

$$f_{P_0}(j^{(d)}) = 0, \tag{H}$$

alors f_{P_0} n'est pas une immersion formelle en $P_0(\mathbb{F}_\ell)$.

(Si f_{P_0} était une immersion formelle en $P_0(\mathbb{F}_\ell)$, en effet, les points $j^{(d)}$ et P_0 seraient égaux (voir 4.13 de [22]), or $j^{(d)}$ est par définition non cuspidal.) La suite de la méthode de Mazur exposée ici va consister alors à tenter de construire une variété abélienne A et, pour chaque diviseur cuspidal P_0 qui peut intervenir plus haut, un morphisme f_{P_0}, qui vérifie l'hypothèse (H) et qui est une immersion formelle en $P_0(\mathbb{F}_\ell)$. Lorsqu'on parvient à construire les f_{P_0}, on élimine la possibilité de réduction multiplicative déployée pour tout $\mathcal{E}$ comme ci-dessus, et on majore donc p en fonction de ℓ.

Pour satisfaire à l'hypothèse (H) de la méthode de Mazur, il est naturel de prendre pour A une variété de rang nul sur $\mathbb{Q}$: en attendant

d'être nuls, les points $f_{P_0}(j^{(d)})$ seront automatiquement de torsion. Pour cela, considérons le quotient d'enroulement de $J_1(p)$, qu'on définit comme pour $J_0(p)$ (voir [22]) — rappelons brièvement comment. On considère le premier groupe d'homologie singulière relative aux pointes de $X_1(p)(\mathbb{C})$: $H_1(X_1(p)(\mathbb{C}), \text{pointes}; \mathbb{Z})$. Si a et b sont deux éléments de $\mathbb{P}^1(\mathbb{Q})$, le symbole modulaire $\{a, b\}$ est l'élément de $H_1(X_1(p)(\mathbb{C}), \text{pointes}; \mathbb{Z})$ défini par l'image de n'importe quel chemin continu reliant a à b sur le demi-plan de Poincaré auquel on a ajouté l'ensemble $\mathbb{P}^1(\mathbb{Q})$ de ses pointes. On a un isomorphisme d'espaces vectoriels réels :

$$H_1\big(X_1(p)(\mathbb{C})\,;\,\mathbb{Z}\big) \otimes \mathbb{R} \simeq \mathrm{Hom}_{\mathbb{C}}\big(H^0(X_1(p)_{\mathbb{C}}\,;\,\Omega^1), \mathbb{C}\big),$$

que définit l'intégration. L'image réciproque par cet isomorphisme de la forme linéaire « intégration le long de $\{0, \infty\}$ » est appelée *l'élément d'enroulement*, noté e ; il est à coefficients dans $\mathbb{Q}$ selon un théorème de Manin et Drinfeld (voir [4]). Pour tout entier n, et tout entier m premier à p, on définit classiquement la correspondance de Hecke $\widetilde{T_n}$ et la correspondance losange $\widetilde{\langle m \rangle}$ (voir par exemple [3], 3, 7.3 et 8.3) qui définissent des opérateurs T_n et $\langle m \rangle$ sur $H_1(X_1(p)(\mathbb{C}), \text{pointes}; \mathbb{Z})$. Ces correspondances définissent aussi des endomorphismes (encore notés T_n et $\langle m \rangle$) de $J_1(p)_{\mathbb{Q}}$; on note $\mathbb{T}_{\Gamma_1(p)}$ la sous-algèbre de $\mathrm{End}(J_1(p))$ engendrée par les T_n et $\langle m \rangle$. (Si $\widetilde{A}$ est un polynôme en les $\widetilde{T_n}$ et $\widetilde{\langle m \rangle}$, on note A son image dans l'algèbre de Hecke $\mathbb{T}_{\Gamma_1(p)}$.) Cette algèbre agit sur les objets qui se déduisent de $J_1(p)$, comme $H^0(X_1(p)_{\mathbb{C}}\,;\,\Omega^1)$ ou $H_1(X_1(p)(\mathbb{C})\,;\,\mathbb{Z})$. Notons $\mathcal{A}_e$ l'idéal annulateur dans $\mathbb{T}_{\Gamma_1(p)}$ de e. Le *quotient d'enroulement* J_1^e est la variété abélienne quotient $J_1(p)/\mathcal{A}_e J_1(p)$.

Les résultats sur la conjecture de Birch et Swinnerton-Dyer, annoncés par Kato [10], mais non encore publiés — voir cependant [26] et [25] —, permettraient d'obtenir l'énoncé suivant :

1.6. CONJECTURE. — *Le rang de $J_1^e(\mathbb{Q})$ est nul.*

(C'est l'assertion $(*)_p$ de la section précédente. Dans le cas de $J_0(N)$ pour N un entier quelconque, cette conjecture est un théorème (voir [22], 3.9) grâce aux travaux de Kolyvagin, Logachev *et al.* ; on renvoie à la section 2.1 de cet article pour plus de précisions.) Dans la suite de cette section, on supposera cette conjecture vraie, au moins pour $p \in \{17, 19, 23, 29, 31, 37, 43\}$. Pour vérifier l'hypothèse (H), on a besoin du résultat suivant (montré en 2.2).

1.7. LEMME. — *Soit ℓ un nombre premier, A un $\mathbb{Z}_{(\ell)}$-schéma en groupes de section neutre 0, P un point de A à valeurs dans $\mathbb{Z}_{(\ell)}$ tel que P soit de torsion, et $P_{\mathbb{F}_\ell} = 0_{\mathbb{F}_\ell}$. Si $\ell > 2$, $P = 0$; si $\ell = 2$ et $P \neq 0$, alors P engendre un $\mu_{2/\mathbb{Z}_{(2)}}$.*

Maintenant notons $\mathcal{A}_e^\perp$ l'idéal de $\mathbb{T}_{\Gamma_1(p)}$ qui annule $\mathcal{A}_e$, et donnons-nous deux éléments de $\mathbb{T}_{\Gamma_1(p)}$: t_1 appartenant à $\mathcal{A}_e^\perp$, et t_2 valant 1 si $\ell > 2$, annulant tout μ_2 immergé dans $J_1(p)_{\mathbb{Z}_{(2)}}$ si $\ell = 2$; considérons le morphisme f_{P_0} :

$$\begin{aligned} X_1(p)^{(d)} &\longrightarrow J_1(p) &&\longrightarrow J_1(p), \\ Q &\longmapsto (Q - P_0) &&\longmapsto t_1 \cdot t_2(Q - P_0). \end{aligned}$$

La seconde flèche se factorise par $J_1(p) \to J_1^e$, et le lemme précédent montre que f_{P_0} vérifie l'hypothèse (H) de la méthode de Mazur. (Ici se manifeste implicitement une nouvelle difficulté technique due au fait qu'on veut pouvoir réduire en 2 : si on réduisait en $\ell > 2$, on pourrait considérer plus simplement la flèche quotient $J_1(p) \to J_1^e$ (au lieu de multiplier par t_1), et en déduire par des résultats de Raynaud une injection sur les espaces tangents correspondants qu'on utiliserait dans le critère 2.7 (voir 1.10). Mais ces résultats de Raynaud ne s'appliquent pas en 2 (voir [22], section 4.8).)

Les propositions techniques suivantes, montrées en 2.4 et 2.5, permettent de construire des éléments t_1 et t_2 comme ci-dessus.

1.8. PROPOSITION. — *Si q est un nombre premier différent de p, alors $a_q := (T_q - q\langle q\rangle - 1)$ annule la torsion $\mathbb{Q}$-rationnelle d'ordre premier à pq de $J_1(p)$, et $A_q := (T_q - q\langle q\rangle - 1)\cdot(T_q - \langle q\rangle - q)$ envoie $H_1(X_1(p)(\mathbb{C}), \text{pointes}; \mathbb{Z})$ sur $H_1(X_1(p)(\mathbb{C}); \mathbb{Z})$.*

1.9. LEMME. — *Avec les notations qui précèdent, soit t un élément de $\mathbb{T}_{\Gamma_1(p)}$, et $P(X) = \prod_{i=1}^n P_i(X)$ son polynôme minimal sur $\mathbb{Q}$ décomposé en facteurs irréductibles; supposons que $P(X)$ est de degré $\dim_{\mathbb{Q}}(\mathbb{T}_{\Gamma_1(p)} \otimes \mathbb{Q})$. Notons $I = \{j \in \mathbb{N} \mid (P/P_j)(t) \cdot e = 0\}$. Alors $t_1 := \prod_{j\in I} P_j(t)$ est élément de $\mathcal{A}_e^\perp$. De plus l'ensemble $J = \{j \in \mathbb{N} \mid (P/P_j)(t)(\widetilde{A}_q \cdot \{0, \infty\}) = 0\}$ contient I.*

Il suffit alors de donner un critère permettant de savoir si un morphisme f_{P_0} comme ci-dessus est immersion formelle en $P_0(\mathbb{F}_\ell)$: c'est la proposition 2.7, qui est une généralisation du « critère de Kamienny » pour Γ_0. Énonçons ce critère, en résumant toute la méthode qui vient d'être exposée.

1.10. THÉORÈME. — *Soit d un entier, p un nombre premier. Supposons l'hypothèse $(*)_p$ de 1.1 vérifiée. Choisissons un nombre premier ℓ différent de p, et deux éléments t_1 et t_2 de $\mathbb{T}_{\Gamma_1(p)}$, le premier dans $\mathcal{A}_e^{\perp}$, le second égal à 1 si ℓ est différent de 2, et si $\ell = 2$ annulant les μ_2 immergés dans $J_1(p)_{\mathbb{Z}_{(2)}}$. Considérons les familles*

$$\begin{aligned}\big(&t_1 \cdot t_2 T_1,\ t_1 \cdot t_2 T_2, \ldots,\ t_1 \cdot t_2 T_{n_1},\\ &t_1 \cdot t_2\langle d_2\rangle T_1, t_1 \cdot t_2\langle d_2\rangle T_2, \ldots, t_1 \cdot t_2\langle d_2\rangle T_{n_2}, \ldots, \ldots,\\ &t_1 \cdot t_2\langle d_m\rangle T_1,\ t_1 \cdot t_2\langle d_m\rangle T_2, \ldots,\ t_1 \cdot t_2\langle d_m\rangle T_{n_m}\big),\end{aligned}$$

pour toutes les partitions de d en sommes d'entiers positifs : $d = \sum_{i=1}^{m} n_i$, et pour chacune tous les m-uplets $(d_1, d_2, \ldots, d_m)$ avec $1 \leq d_1, \ldots, d_m \leq \frac{1}{2}(p-1)$, les d_i étant deux à deux distincts.

Si $p > (1 + \ell^{d/2})^2$, et si toutes les familles précédentes sont $\mathbb{F}_\ell$-libres dans $\mathbb{T}_{\Gamma_1(p)} \otimes \mathbb{F}_\ell$, alors p n'est pas élément de $S(d)$.

Encore une fois, les propositions 1.8 et 1.9 permettent de construire des t_i comme dans le théorème. Notons par ailleurs que, comme on le démontre en 2.6, la conclusion du théorème reste vraie si on choisit, pour *chaque* famille correspondant à une partition de d, une paire d'opérateurs t_1 et t_2 vérifiant les hypothèses du théorème. La théorie des symboles modulaires permet de ramener la vérification des indépendances linéaires de 1.10 à des calculs qui, pour des petits degrés, sont effectuables, comme on va le montrer dans la suite pour $d = 3$. Explicitons ce que devient la méthode de Mazur dans ce cas.

1.11. Application aux corps cubiques.

Dans le cas des corps cubiques, on va d'abord montrer que $S(3)$ contient $\{2, 3, 5, 7, 11, 13\}$ (on sait que $S(1) = \{2, 3, 5, 7\}$, et on va montrer en 2.8 que $S(3)$ contient 11 et 13). On connaît par ailleurs le majorant d'Oesterlé : si p est élément de $S(3)$, p est inférieur ou égal à 43. Comme on l'a remarqué en 1.1, la réduction en 3 ne permet d'éliminer que 43 ; on va donc réduire en 2. Soit p un nombre premier parmi $\{19, 23, 29, 31, 37, 43\}$. Pour tout triplet de pointes P_0 de $X_1(p)^{(3)}$, P_0 étant d'image $\infty^{(3)}$ dans $X_0(p)^{(3)}$, on construira un morphisme f_{P_0}, en exhibant un élément t_1 de $\mathcal{A}_e^{\perp}$ (1.9), et en prenant pour t_2 un opérateur de type a_n (1.8). Si on suppose vraie l'assertion $(*)_p$ de 1.1 pour $17 \leq p \leq 43$, tous ces morphismes vérifieront l'hypothèse (H) de la méthode de Mazur. Pour montrer que ces morphismes sont des immersions formelles en $P_0(\mathbb{F}_\ell)$, on utilisera le critère suivant.

1.12. PROPOSITION (critère de Kamienny cubique). — *Avec les notations de* 1.10, *si les familles*

- $(t_1 \cdot t_2 \cdot T_1, t_1 \cdot t_2 \cdot T_2, t_1 \cdot t_2 \cdot T_3)$,
- $(t_1 \cdot t_2 \cdot T_1, t_1 \cdot t_2 \cdot \langle d \rangle, t_1 \cdot t_2 \cdot T_2)$, *et*
- $(t_1 \cdot t_2 \cdot T_1, t_1 \cdot t_2 \cdot \langle d_1 \rangle, t_1 \cdot t_2 \cdot \langle d_2 \rangle)$

sont toutes libres dans $\mathbb{T}_{\Gamma_1(p)} \otimes \mathbb{F}_\ell$ (*avec* $1 < d, d_1, d_2 < \frac{1}{2}p$, *et* $d_1 < d_2$), *alors chaque morphisme* f_{P_0} *est une immersion formelle en* $P_0(\mathbb{F}_\ell)$.

Ce critère sera vérifié pour les p énumérés plus haut, avec des calculs explicites pour 19 (4.2), par des calculs sur ordinateur pour les autres (section 5) ; ce qui les exclura de $S(3)$. Restera enfin le cas de 17, discuté dans la section 4.3.

2. Preuve des résultats énoncés dans la section 1.

2.1. À propos de 1.6.

Dans [22], théorème 3.9, on montre que le quotient d'enroulement de $J_0(N)$ sur $\mathbb{Q}$ est de rang nul (N quelconque). Dans le cas de $J_1(p)$, on a de même une isogénie :

$$J_1(p)_{\mathbb{Q}} \longrightarrow \oplus_{G_{\mathbb{Q}} \cdot f}(J_f),$$

où la somme est prise sur les orbites sous l'action de Galois de toutes les formes nouvelles en niveau p. Avec les notations de 2.6, le théorème 3.5 de [22] permet d'écrire $\mathcal{A}_e \otimes \mathbb{Q} = \bigoplus_{G_{\mathbb{Q}} f / L(f,1)=0} R_f$, puisque $L(f,1) = 2\pi\langle e, f\rangle$. On en déduit des morphismes :

$$J_1^e(\mathbb{Q}) = \big(J_1(p)/\mathcal{A}_e J_1(p)\big)(\mathbb{Q}) \longrightarrow \prod_{R_f \not\subset \mathcal{A}_{e,\mathbb{Q}}} \big(J_1(p)/(\mathbb{T}_{\Gamma_1(p),\mathbb{Q}}/R_f)J_1(p)\big)(\mathbb{Q}) \longrightarrow \prod_{G_{\mathbb{Q}} f / L(f,1) \neq 0} J_f(\mathbb{Q}).$$

Dans la décomposition équivalente de J_0, on sait par un théorème de Kolyvagin-Logachev que ces J_f à fonction L non nulle en 1 sont de rang nul sur $\mathbb{Q}$. Pour J_1, ce n'est pas encore prouvé (voir pourtant [10], et [25]).

2.2. Preuve de 1.7.

On prouve plus généralement :

2.3. PROPOSITION. — *Soit R un anneau de valuation discrète v d'inégales caractéristiques, de corps de fractions K et de corps résiduel k de caractéristique ℓ. Soit r un élément de R, de valuation non nulle. Soit G un R-schéma en groupes de section neutre e, et P un point de torsion de $G(R)$ tel que $P = e$ dans $G(R/rR)$. Alors l'ordre de P est une puissance ℓ^n de ℓ, et $v(\ell) \geq \phi(\ell^n) \cdot v(r)$ (ϕ désignant l'indicateur d'Euler). En particulier, si on a $\ell = 2$, R non ramifié, $P_k = e_k$ et $P \neq e$, alors P est d'ordre 2; de plus dans ce cas la réunion de P et e est un sous-schéma en groupes, isomorphe à μ_2.*

Cette proposition, dont la preuve est dans l'esprit de [6], exposé IX, 4.7.1 est une généralisation du lemme 4.14 de [22], et une variante de résultats de Raynaud (voir par exemple le théorème 3.3.3 de [Raynaud]). On peut supposer R complet. Notons N l'ordre de P. Choisissons un voisinage affine V de $e(k)$. Soit H_K le fermé de la fibre générique de G défini par l'union des multiples de P_K, et H son adhérence schématique dans V. La preuve du lemme 4.14 de [22] montre que H est un schéma en groupes affine (dont on notera $\mathcal{H}$ l'anneau des coordonnées) qui est commutatif, fini et libre sur R, de rang N. Si N était premier à ℓ, H serait étale sur R; on en déduit, en considérant un multiple convenable de P, que N est une puisance ℓ^n de ℓ. Si $n = 0$, l'énoncé est trivial : supposons $n > 0$. L'action du schéma en groupes H sur lui-même par translation fournit un morphisme de R-schémas en groupes : $H \to \mathrm{GL}_{\ell^n,R}$. L'image de P dans $\mathrm{GL}_{\ell^n}(R)$ obtenue *via* ce morphisme permet de voir $\mathcal{H}$ comme un module sur $R[X]/(X^{\ell^n} - 1)$. Soit K' une extension finie de K qui contient une racine de l'unité d'ordre ℓ^n, qu'on notera ζ_{ℓ^n} ; soit R' la clôture intégrale de R dans K'. Soit $\mathcal{H}'$ le quotient de $\mathcal{H} \otimes_{R[X]/(X^{\ell^n}-1)} R'$ par sa partie de R'-torsion; c'est un module libre non nul sur R'. Comme $P = e$ dans $G(R/rR)$, on a $(\zeta_{\ell^n} - 1) = 0$ dans R'/rR', et donc $v(r) \leq v(\zeta_{\ell^n} - 1) = v(\ell)/\phi(\ell^n)$. Supposons enfin $\ell = 2$, R non ramifié en 2, $P_k = e_k$ et $P \neq e$; P est d'ordre 2 par ce qui précède. De plus, pour tout R-schéma en groupes H' de rang 2 sur R il y a une flèche canonique $(\mathbb{Z}/2\mathbb{Z})_R \to H'_R$. En passant par les duaux de Cartier, on voit que l'application canonique $(\mathbb{Z}/2\mathbb{Z})_R \to (\mu_2)_R$ se factorise par H. Or l'algèbre de $(\mu_2)_R$ est de co-longueur 1 dans celle de $(\mathbb{Z}/2\mathbb{Z})_R$: donc $H_R \simeq (\mu_2)_R$. □

2.4. Preuve de 1.8.

Soit n un entier premier à pq, et P un élément de $J_1(p)_{\mathbb{F}_q}(\mathbb{F}_q)[n]$. Le Frobenius absolu F_q de la fibre de $J_1(p)$ en q et son isogénie duale V_q (Verschiebung) vérifient les relations : $F_q + \langle q \rangle V_q = T_q$ (Eichler-Shimura),

et $F_q \cdot V_q = q$. Donc $T_q(P) = P + \langle q \rangle V_q(P) = (1 + q \cdot \langle q \rangle)(P)$. Puisque la n-torsion de $J_1(p)$ est finie étale sur $\mathbb{Z}[1/pn]$, l'opérateur a_q annule la n-torsion $\mathbb{Q}$-rationnelle de $J_1(p)$, ce qui est la première assertion.

Pour la seconde, utilisons le lemme de Cremona (3.7) pour choisir un système de représentants dans $\mathbb{P}^1(\mathbb{Q})$ des pointes sur $\mathbb{C}$, par exemple $\{\binom{1}{a}, 1 \leq a \leq \frac{1}{2}(p-1)\} \cup \{\binom{a}{p}, 1 \leq a \leq (p-1)/2\}$ (le premier ensemble est celui des pointes au-dessus de 0 dans $X_0(p)$, le second celui au-dessus de ∞). La correspondance de Hecke $\widetilde{T_q}$ agit sur ces diviseurs par multiplication à gauche par les matrices suivantes (voir [3], 3.4.1) :

$$\widetilde{T_q} = \Big(\sum_{\alpha=0}^{q-1} \begin{pmatrix} 1 & \alpha \\ 0 & q \end{pmatrix}\Big) + \sigma_q \begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix},$$

où σ_q est un élément de $\mathrm{SL}_2(\mathbb{Z})$ congru à $\left(\begin{smallmatrix} \bar{q} & 0 \\ 0 & q \end{smallmatrix}\right)$ mod (p) (pour x un entier, on désigne par $\bar{x}$ un autre entier congru à l'inverse de x mod (p)). Remarquons que sur le système choisi de pointes, on a pour action des correspondances losanges :

$$\widetilde{\langle d \rangle} \cdot \binom{1}{a} = \binom{1}{d \cdot a} \quad \text{et} \quad \widetilde{\langle d \rangle} \cdot \binom{a}{p} = \binom{\bar{d} \cdot a}{p}.$$

On vérifie alors facilement (en distinguant selon que a est premier ou non à p) que

$$\widetilde{T_q} \cdot \binom{1}{a} = (q\widetilde{\langle q \rangle} + 1) \cdot \binom{1}{a} \quad \text{et} \quad \widetilde{T_q} \cdot \binom{a}{p} = \Big(\widetilde{\langle q \rangle} + q\Big) \cdot \binom{a}{p}. \qquad \square$$

2.5. Preuve de 1.9.

En niveau premier, l'algèbre de Hecke tensorisée par $\mathbb{Q}$ s'écrit comme un produit $\mathbb{T}_{\Gamma_1(p)} \otimes \mathbb{Q} = \prod_{i=1}^{k} R_i$, où les R_i sont des corps de nombres (théorème 3.5 de [22]) (ce qui implique que les racines de P sont toutes distinctes) ; et $\mathcal{A}_e \otimes \mathbb{Q} = \prod_{i \in I} R_i$, $\mathcal{A}_e^{\perp} \otimes \mathbb{Q} = \prod_{j \notin I} R_j$. D'où la première assertion.

L'élément $A_q \cdot \{0, \infty\}$ de $H_1(X_1(p)(\mathbb{C}), \text{pointes} ; \mathbb{Z})$ est de bord nul, par la proposition 1.8. Il définit par l'intégration la même forme linéaire que $A_q \cdot e \in H_1(X_1(p)(\mathbb{C}) ; \mathbb{Q})$; donc ces éléments, appartenant à $H_1(X_1(p)(\mathbb{C}) ; \mathbb{Z})$, sont égaux. D'où la seconde assertion. $\square$

2.6. Preuve de 1.10.

Étant donnés les résultats de la section 1.5, il suffit de montrer la proposition 2.7, qui est une généralisation du «critère de Kamienny». Plaçons-nous dans une situation un peu plus générale qu'en 1.5. Soit ℓ un nombre premier, N un entier premier à ℓ, et P_0 un point de $X_1(N)^{(d)}(\mathbb{Z}_{(\ell)})$ qui s'écrit sous la forme : $P_0 = \sum_{i=1}^{m} n_i P_{0,i}$, les $P_{0,i}$ étant des pointes à valeurs dans $\mathbb{Z}_{(\ell)}$ deux à deux distinctes, d'image $\infty_{\mathbb{Z}_{(\ell)}}$ dans $X_0(N)_{\mathbb{Z}_{(\ell)}}$. Comme on le voit avec l'interprétation modulaire des $P_{0,i}$ donnée en 1.5, ces pointes sont conjuguées sous l'action des opérateurs losanges : pour chaque entier j inférieur à m, désignons par d_j un entier tel que $P_{0,1} = \langle d_j \rangle \cdot P_{0,j}$. Soit t un élément de $\mathbb{T}_{\Gamma_1(N)}$; notons f_{P_0} le morphisme $X_1(N)^{(d)} \to J_1(N)$ construit comme en 1.5, qui à un point Q associe $t \cdot (Q - P_0)$.

2.7. PROPOSITION. — *Avec les notations qui précèdent, f_{P_0} est une immersion formelle en $P_0(\mathbb{F}_\ell)$ si et seulement si la famille*

$$\begin{aligned}\big(t \cdot T_1,\ t \cdot T_2, \ldots,\ t \cdot T_{n_1},\ t \cdot \langle d_2 \rangle T_1,\ t \cdot \langle d_2 \rangle T_2, \ldots,\ t \cdot \langle d_2 \rangle T_{n_2}, \ldots,\\ \ldots,\ t \cdot \langle d_m \rangle T_1,\ t \cdot \langle d_m \rangle T_2, \ldots,\ t \cdot \langle d_m \rangle T_{n_m}\big)\end{aligned}$$

est $\mathbb{F}_\ell$-libre dans $\mathbb{T}_{\Gamma_1(N)} \otimes \mathbb{F}_\ell$.

Preuve (*cf.* [22], (4.16), (4.17), (4.18).). — Il suffit de prouver que l'hypothèse de la proposition est équivalente à ce que l'application tangente à f_{P_0} en $P_0(\mathbb{F}_\ell)$ soit injective. On va donc montrer que la famille de la proposition est l'image par l'application tangente à f_{P_0} d'une base de l'espace tangent à $X_1(N)^{(d)}_{\mathbb{F}_\ell}$ en $P_0(\mathbb{F}_\ell)$. Dans la suite, on désignera $P_0(\mathbb{F}_\ell)$ (respectivement $P_{0,i}(\mathbb{F}_\ell)$) par $\widetilde{P}_0$ (respectivement $\widetilde{P}_{0,i}$). Si q est une coordonnée formelle de la courbe $X_1(N)_{\mathbb{F}_\ell}$ en $\widetilde{P}_{0,1}$, $X_1(N)_{\mathbb{F}_\ell}$ a la coordonnée formelle $\langle d_j \rangle^* q$ au point $\widetilde{P}_{0,j}$, donc $X_1(N)^d_{\mathbb{F}_\ell}$ a les coordonnées formelles $q_1, \ldots, q_{n_1}, (\langle d_2 \rangle^* q)_1, \ldots, (\langle d_2 \rangle^* q)_{n_2}, \ldots (\langle d_m \rangle^* q)_1, \ldots, (\langle d_m \rangle^* q)_{n_m}$ au point $(\widetilde{P}_{0,1}, \ldots, \widetilde{P}_{0,m})$, et $X_1(N)^{(d)}_{\mathbb{F}_\ell}$ a comme coordonnées formelles en $\widetilde{P}_0$ les

$$\sigma_1(q_1, \ldots, q_{n_1}), \sigma_2(q_1, \ldots, q_{n_1}), \ldots, \sigma_{n_1}(q_1, \ldots, q_{n_1}),$$

$$\sigma_1((\langle d_2 \rangle^* q)_1, \ldots, (\langle d_2 \rangle^* q)_{n_2}), \ldots, \sigma_{n_2}((\langle d_2 \rangle^* q)_1, \ldots (\langle d_2 \rangle^* q)_{n_2}),$$

$$\ldots,$$

$$\sigma_1((\langle d_m \rangle^* q)_1, \ldots, (\langle d_m \rangle^* q)_{n_m}), \ldots, \sigma_{n_m}((\langle d_m \rangle^* q)_1, \ldots, (\langle d_m \rangle^* q)_{n_m}),$$

(on a noté $\sigma_j(x_1,\dots,x_k)$ le j-ième polynôme symétrique élémentaire en k variables, somme de tous les produits de j variables distinctes). Notons $(s_i^{n_j}), 1 \leq j \leq m, 1 \leq i \leq n_j$ ce système de coordonnées formelles : les $ds_i^{n_j}$ forment une base de $\mathrm{Cot}_{\widetilde{P}_0}(X_1(N)^{(d)}_{\mathbb{F}_\ell})$. Soit F l'application naturelle $X_1(N) \to J_1(N)$, normalisée par $P_{0,1} \mapsto 0$, et pour tout élément ω de $\mathrm{Cot}_{0_{\mathbb{F}_\ell}}(J_1(N)_{\mathbb{F}_\ell})$, notons $(\sum_{n\geq 1} a_n(\omega)q^n)(dq/q)$ le développement de Fourier en $\widetilde{P}_{0,1}$ de la forme différentielle $F^*(\omega)$ sur $X_1(N)_{\mathbb{F}_\ell}$.

Considérons la composition de morphismes :

$$X_1(N)^d \xrightarrow{\Phi} X_1(N)^{(d)} \xrightarrow{f_{P_0}} J_1(N)$$

avec Φ le morphisme canonique, et posons $S_n(x_1,\dots,x_k) = \sum_{i=1}^k x_i^n$ pour tout entier n et tout k-uplet d'indéterminées $(x_1,\dots,x_k)$. Soit $\omega \in \mathrm{Cot}_{0_{\mathbb{F}_\ell}}(J_1(N)_{\mathbb{F}_\ell})$; le développement de Fourier de $\Phi^* \cdot f_{P_0}^*(\omega)$ en $(\widetilde{P}_{0,1},\dots,\widetilde{P}_{0,m})$ est :

$$\Phi^* \cdot f_{P_0}^*(\omega) = \sum_{j=1}^m \sum_{n\geq 1} a_n\big(\langle d_j\rangle \cdot t \cdot \omega\big) n^{-1} dS_n\big((\langle d_j\rangle^* q)_1,\dots,(\langle d_j\rangle^* q)_{n_j}\big).$$

Les relations de Newton donnent

$$\sum_{j=0}^n (-1)^j S_j(x_1,\dots,x_k)\cdot \sigma_{n-j}(x_1,\dots,x_k) = 0$$

(pour tout n compris entre 1 et k), d'où

$$n^{-1} dS_n\big((\langle d_j\rangle^* q)_1,\dots,(\langle d_j\rangle^* q)_{n_j}\big) = (-1)^{n-1} d\sigma_n\big((\langle d_j\rangle^* q)_1,\dots,(\langle d_j\rangle^* q)_{n_j}\big)$$

(pour tout n compris entre 1 et n_j). On en déduit donc l'égalité dans $\mathrm{Cot}_{\widetilde{P}_0}(X_1(N)^{(d)}_{\mathbb{F}_\ell})$:

$$f_{P_0}^*(\omega) = \sum_{j=1}^m \big(a_1(\langle d_j\rangle \cdot t \cdot \omega) ds_1^{n_j} - a_2(\langle d_j\rangle . t \cdot \omega) ds_2^{n_j} + \cdots + (-1)^{n_j-1} a_{n_j}(\langle d_j\rangle \cdot t \cdot \omega) ds_{n_j}^{n_j}\big).$$

Le fait qu'on soit en des pointes de $X_1(N)$ au-dessus de $\infty \in X_0(N)$ (la «convention cruciale» mentionnée en 1.5, juste avant «Méthode de Mazur») entraîne la relation $a_1(T_n f) = a_n(f)$ pour tout n et toute forme modulaire (voir [28], 3.5.12); ce qui permet de déduire de l'égalité précédente que l'application tangente à f_{P_0} en $\widetilde{P}_0$ envoie $d/ds_i^{n_j}$ sur $(-1)^{i-1} t \cdot \langle d_j\rangle T_i(\frac{\mathrm{d}}{\mathrm{d}q}|_{0_{\mathbb{F}_\ell}})$. Or $\mathrm{Tan}_{0_{\mathbb{F}_\ell}}(J_1(N)_{\overline{\mathbb{F}}_\ell})$ est un $\mathbb{T}_{\Gamma_1(N)} \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_\ell$-module libre de rang 1 de base $\frac{\mathrm{d}}{\mathrm{d}q}|_{0_{\mathbb{F}_\ell}}$ (cela se montre exactement de la même façon que pour J_0, pour laquelle c'est fait par exemple en 4.2 de [22]). □

2.8. Existence de torsion cubique d'ordre 11 et 13.

Montrons d'abord que $X_1(11)$ possède une infinité de points à valeurs dans des corps cubiques. Cette courbe modulaire est une courbe elliptique sur $\mathbb{Q}$ (puisque propre, lisse, géométriquement connexe, de genre 1 (voir 4.1), munie d'un point (une des pointes rationnelles par exemple)) et possède donc une équation de Weierstrass. La fonction y donne un morphisme : $X_1(11) \to \mathbb{P}^1$, de degré 3. Or le théorème de Hilbert assure que $\mathbb{Q}$ est hilbertien, *i.e.* $\mathbb{P}^1(\mathbb{Q})$ n'est pas mince (voir [27], chap. 9). Ce qui signifie qu'il existe un sous-ensemble de $\mathbb{P}^1(\mathbb{Q})$ dans le complémentaire infini duquel chaque point $\mathbb{Q}$-rationnel se relève en un point fermé de degré 3 de $X_1(11)$ (voir [27], 9.2, prop. 1). (Bien sûr, comme me l'a fait remarquer Ph. Satgé, on peut aussi invoquer le théorème de Mazur sur $S(1)$!)

Considérons maintenant l'action du groupe des opérateurs losanges, isomorphe à $\mathbb{F}_{13}^*/(\pm 1) \simeq \mathbb{Z}/6\mathbb{Z}$, sur $X_1(13)$. Le quotient de cette courbe par le sous-groupe d'ordre 3 du groupe des losanges, $X_1(13)/(\mathbb{Z}/3\mathbb{Z})$, est de genre nul, comme on le calcule avec la formule de Hurwitz (on le voit d'ailleurs directement dans les tables de [13], en constatant qu'aucune forme propre de $S_2(X_1(13), \mathbb{C})$ n'est stable par $(\mathbb{Z}/3\mathbb{Z})$). Comme il possède un point rationnel, il est isomorphe à $\mathbb{P}^1_{\mathbb{Q}}$. Le degré du morphisme naturel de $X_1(13)$ vers ce quotient étant 3, on conclut comme plus haut.

Remarque. — Comme on l'a déjà remarqué en introduction, on trouve dans [23] des paramétrisations de courbes elliptiques (à j-invariant entier au-dessus de 2, 3, ou 5) ayant de la 11 ou 13-torsion sur des corps cubiques.

3. Résultats sur les symboles modulaires pour Γ_1.

3.1. Présentation de Manin.

Pour vérifier par le calcul (éventuellement sur ordinateur) le critère 2.7, *i.e.* l'hypothèse d'indépendance linéaire de 1.10, on a besoin d'expliciter l'espace $\mathrm{Tan}_{0_{\mathbb{F}_\ell}}(J_1(p)_{\mathbb{F}_\ell})$. Or cet espace est un $\mathbb{T}_{\Gamma_1(p)} \otimes \mathbb{F}_\ell$-module libre de rang 1, et on a par ailleurs une représentation fidèle de $\mathbb{T}_{\Gamma_1(p)}$ dans $H_1(X_1(p)(\mathbb{C}) ; \mathbb{Z})$ (voir 1.5). On se sert donc, pour calculer l'espace tangent, de la présentation de Manin de cet espace d'homologie, pour laquelle on doit donner un relèvement de l'action de générateurs de $\mathbb{T}_{\Gamma_1(p)}$ (opérateurs de Hecke T_n et opérateurs losanges) ; on trouve ces résultats par exemple dans [18] (voir aussi [1], où des calculs sur les symboles modulaires pour Γ_1

sont décrits. Signalons cependant que les nôtres sont un peu différents, en particulier pour ce qui est des opérateurs de Hecke : Cremona calcule leur action directement sur l'homologie, alors que nous travaillons dans l'espace engendré par les symboles (théorème 3.4)).

Rappelons quelques faits et notations. Soit $\mathcal{G}$ un sous-groupe d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$; on peut définir sur $\mathbb{C}$ la courbe $X_{\mathcal{G}}$, et ses symboles modulaires comme en 1.5. Notons $R_{\mathcal{G}}$ un système de représentants des classes à droite de $\mathcal{G}$ dans $\mathrm{SL}_2(\mathbb{Z})$. On considère $H_1(X_{\mathcal{G}}\,;\mathbb{Z})$ comme un sous-groupe (noyau de l'application « bord ») de $H_1(X_{\mathcal{G}}, \text{pointes}\,;\mathbb{Z})$. On note ξ le morphisme de groupes de $\mathbb{Z}[R_{\mathcal{G}}]$ dans $H_1(X_{\mathcal{G}}, \text{pointes}\,;\mathbb{Z})$ qui au représentant $g = (a,b\,;c,d)$ d'une classe de $\mathcal{G}\backslash SL_2(\mathbb{Z})$ associe $\{g\cdot 0, g\cdot\infty\} = \{b/d, a/c\}$. (On peut définir ξ sur tout $\mathrm{GL}_2(\mathbb{Q})$, comme on le fera dans le théorème 3.4.) Notons $\sigma := (0,1\,;-1,0)$ et $\tau := (0,-1\,;1,-1)$ les habituels générateurs de $\mathrm{SL}_2(\mathbb{Z})$, qu'on fait agir sur $R_{\mathcal{G}}$ à droite. On désignera par $\mathbb{Z}[R_{\mathcal{G}}]^\sigma$ (resp. $\mathbb{Z}[R_{\mathcal{G}}]^\tau$) l'ensemble des éléments de $\mathbb{Z}[R_{\mathcal{G}}]$ stables par l'opération de σ (resp. τ). Notons $\delta : \mathbb{Z}[R_{\mathcal{G}}] \to \mathbb{Z}^{\{\text{pointes}\}}$ l'opération « bord », qui associe au représentant $g = (a,b\,;c,d)$ d'une classe de $\mathcal{G}\backslash SL_2(\mathbb{Z})$ l'élément $(b/d) - (a/c)$ de $\mathcal{G}\backslash\mathbb{P}^1(\mathbb{Q})$. Notons $\xi_0 : \mathrm{Ker}(\delta) \to H_1(X_{\mathcal{G}}\,;\mathbb{Z})$ la restriction de ξ à $\mathrm{Ker}(\delta)$; $\mathbb{Z}[R_{\mathcal{G}}]^\sigma$ et $\mathbb{Z}[R_{\mathcal{G}}]^\tau$ appartiennent à $\mathrm{Ker}(\delta)$.

3.2. THÉORÈME (présentation de Manin). — *Les suites*

$$\mathbb{Z}[R_{\mathcal{G}}]^\sigma \times \mathbb{Z}[R_{\mathcal{G}}]^\tau \xrightarrow{+} \mathbb{Z}[R_{\mathcal{G}}] \xrightarrow{\xi} H_1(X_{\mathcal{G}}, \text{pointes}\,;\mathbb{Z}) \to 0$$

et

$$\mathbb{Z}[R_{\mathcal{G}}]^\sigma \times \mathbb{Z}[R_{\mathcal{G}}]^\tau \xrightarrow{+} \mathrm{Ker}(\delta) \xrightarrow{\xi_0} H_1(X_{\mathcal{G}}\,;\mathbb{Z}) \to 0$$

sont exactes.

(C'est le théorème 1.9 de [14].) Dans le cas où $\mathcal{G} = \Gamma_1(N)$ pour un entier N, on choisit $R_{\mathcal{G}}$ égal à

$$\mathcal{P}(\mathbb{Z}/N\mathbb{Z}) = \{x \in (\mathbb{Z}/N\mathbb{Z})^2 \mid x \text{ est d'ordre } N\}/(\pm 1),$$

grâce à la bijection

$$\Gamma_1(N)\begin{pmatrix} a & b \\ c & d\end{pmatrix} \longmapsto (\bar{c},\bar{d}) \equiv (c,d) \bmod (N).$$

Soit $(\bar{c},\bar{d}) \in \mathcal{P}(\mathbb{Z}/N\mathbb{Z})$, et $\Gamma_1(N)(a,b\,;c,d)$ la classe correspondante ; on pose

$$\xi_1(\bar{c},\bar{d}) = \left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix}\cdot 0, \begin{pmatrix} a & b \\ c & d\end{pmatrix}\cdot\infty\right\} = \left\{\frac{b}{d}, \frac{a}{c}\right\},$$

et on en déduit une application

$$\xi_1 : \mathbb{Z}[\mathcal{P}(\mathbb{Z}/N\mathbb{Z})] \longrightarrow H_1\big(X_1(N)(\mathbb{C}), \text{pointes}\,;\,\mathbb{Z}\big)$$

par $\mathbb{Z}$-linéarité. L'application ξ_1 définie sur $\mathbb{Z}[\mathcal{P}(\mathbb{Z}/N\mathbb{Z})]$ s'identifie donc avec l'application ξ précédemment définie sur des matrices.

Relevons maintenant les opérateurs de Hecke et les losanges sur cette présentation.

3.3. Relèvement des opérateurs de Hecke.

Fixons pour toute cette partie un entier N (le niveau). Pour n entier notons, comme dans [3],

$$\Delta_1^n(N) = \left\{ M \in M_2(\mathbb{Z}) \mid \det(M) = n > 0,\ M \equiv \begin{pmatrix} 1 & * \\ 0 & n \end{pmatrix} \bmod (N) \right\},$$

$$\Delta_1'(N) = \bigcup_{\substack{n>0,\\ n \text{ premier à } N}} \Delta_1^n(N).$$

Supposons n premier au niveau N. L'action de l'opérateur de Hecke T_n sur $H_1(X_1(N)(\mathbb{C})\,;\,\mathbb{Z})$ se déduit par linéarité de l'action sur les symboles modulaires : $T_n \cdot \{a,b\} = \sum_{\alpha \in \Gamma_1(N)\backslash\Delta_1^n(N)} \{\alpha\cdot a, \alpha\cdot b\}$ (voir [3], 3.3). Donc si R_n est un ensemble de représentants des classes de $\Gamma_1(N)\backslash\Delta_1^n(N)$, pour tout g de $\mathrm{SL}_2(\mathbb{Z})$, $T_n \circ \xi(g) = \sum_{\alpha\in R_n} \xi(\alpha\cdot g)$. Pour l'opérateur losange $\langle n\rangle$, si on choisit dans $\mathrm{SL}_2(\mathbb{Z})$ un relèvement σ_n de $(n^{-1}, 0\,;\,0, n) \in M_2(\mathbb{Z}/N\mathbb{Z})$, on a, pour tout g de $\mathrm{SL}_2(\mathbb{Z})$, $\langle n\rangle \circ \xi(g) = \xi(\sigma_n \cdot g)$.

Soit $(\overline{w}, \overline{t}) \in \mathcal{P}(\mathbb{Z}/N\mathbb{Z})$ et $(a,b\,;\,c,d) \in \Delta_1^n(N)$ avec n premier à N. Posons

$$(\overline{w}, \overline{t}) \circ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (\overline{aw+tc}, \overline{bw+dt}).$$

On déduit de cela par $\mathbb{Z}$-bilinéarité une application

$$\mathbb{Z}\big[\mathcal{P}(\mathbb{Z}/N\mathbb{Z})\big] \times \mathbb{Z}\big[\Delta_1'(N)\big] \longrightarrow \mathbb{Z}\big[\mathcal{P}(\mathbb{Z}/N\mathbb{Z})\big].$$

Cette application permet d'interpréter les éléments de $\mathbb{Z}[\Delta_1'(N)]$ comme des endomorphismes de $\mathbb{Z}[\mathcal{P}(\mathbb{Z}/N\mathbb{Z})]$ (endomorphismes dont on notera $\circ$ l'action). Soit enfin $\Phi : \Delta_1(N) \to \Gamma_1(N)\backslash SL_2(\mathbb{Z})$ l'application qui à $(a,b\,;\,c,d)$ associe l'élément $\Gamma_1(N)(u,v\,;\,w,t)$ avec $(w,t) = (c,d)$ dans $\mathcal{P}(\mathbb{Z}/N\mathbb{Z})$. Un *relèvement* de l'opérateur T est un élément $\mathcal{T}$ de $\mathbb{Z}[\Delta_1'(N)]$ tel que $T \circ \xi = \xi \circ \mathcal{T}$.

Toujours pour n premier à N, posons $M_2(\mathbb{Z})_n = \Delta_1^n(1)$, l'ensemble des matrices 2×2 à coefficients dans $\mathbb{Z}$ de déterminant n. Soit $S = \sum_M u_M M$ un élément de $\mathbb{Z}[M_2(\mathbb{Z})_n]$; comme dans [18], on dit que S vérifie la condition (C_n) si pour tout $g \in M_2(\mathbb{Z})_n / \mathrm{SL}_2(\mathbb{Z})$, on a, dans $\mathbb{Z}[\mathbb{P}^1(\mathbb{Q})]$, l'égalité

$$\sum_{M \in g} u_M \big((M \cdot \infty) - (M \cdot 0)\big) = (\infty) - (0).$$

3.4. THÉORÈME. — *Soit n un entier premier à N. Tout élément de $\mathbb{Z}[M_2(\mathbb{Z})_n]$ qui vérifie la condition (C_n) est un relèvement de l'opérateur de Hecke T_n, et l'homothétie*

$$D_n = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}$$

est un relèvement de l'opérateur losange $\langle n \rangle$.

Preuve (voir [18], *th.* 2). — Soit $\gamma = (a, b\,;\, c, d)$ dans $\mathrm{SL}_2(\mathbb{Z})$, d'image $(\bar{c}, \bar{d})$ dans $\mathcal{P}(\mathbb{Z}/N\mathbb{Z})$. Pour la seconde assertion, il suffit de remarquer que

$$\langle n \rangle \xi(\gamma) = \xi(\sigma_n \cdot \gamma) = \xi_1\Big((\bar{c}, \bar{d}) \circ \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}\Big) = \xi\Big(\Phi\Big(\gamma \cdot \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}\Big)\Big).$$

Avant de rappeler brièvement comment on démontre la première, montrons comment on peut construire une somme S vérifiant la condition (C_n). Notons $\mathcal{R}_n$ un système de représentants de $M_2(\mathbb{Z})_n / \mathrm{SL}_2(\mathbb{Z})$. Soit g dans $M_2(\mathbb{Z})_n$. La théorie des fractions continues permet de construire une somme S'_g d'éléments de $\mathrm{SL}_2(\mathbb{Z})$, de la forme $\sum_{k=1}^{n_g} g_k$ avec $g_k = (u_k, u_{k+1}\,;\, v_k, v_{k+1})$ pour $1 \leq k \leq n_g$ et $u_1/v_1 = g^{-1} \cdot \infty$, $u_{n_g+1}/v_{n_g+1} = g^{-1} \cdot 0$; *i.e.*

$$\sum_{k=1}^{n_g} \big((g_k \cdot \infty) - (g_k \cdot 0)\big) = (g^{-1} \cdot \infty) - (g^{-1} \cdot 0)$$

(voir par exemple [17], prop. 1). Appelons $S_g = \sum_{M_g} u_{M_g} M_g$ la somme $g \cdot S'_g$. On voit que S_g est une somme d'éléments appartenant tous à la même classe que g dans $M_2(\mathbb{Z})_n / \mathrm{SL}_2(\mathbb{Z})$, tel que $\sum_{M_g} u_{M_g}((M_g \cdot \infty) - (M_g \cdot 0)) = (\infty) - (0)$. On en déduit que la somme sur une famille de représentants de $M_2(\mathbb{Z})_n / \mathrm{SL}_2(\mathbb{Z})$ de tels S_g vérifie la condition (C_n).

Montrons maintenant que toute somme S vérifiant la condition (C_n) est un relèvement de T_n. On peut écrire $S = \sum_{g\in\mathcal{R}_n}\sum_{k=1}^{n_g} gg_k$ comme ci-dessus. Soit γ dans $\mathrm{SL}_2(\mathbb{Z})$. On a :

$$\xi\circ S\circ\big(\Gamma_1(N)\gamma\big) = \sum_{g\in\mathcal{R}_n}\sum_{k=1}^{n_g}\xi\big(\Phi(\gamma gg_k)\big) = \sum_{g\in\mathcal{R}_n}\sum_{k=1}^{n_g}\xi\big(\Phi(\gamma g)g_k\big)$$
$$= \sum_{g\in\mathcal{R}_n}\xi\big(\Phi(\gamma g)g^{-1}\big) \quad = \sum_{g\in\mathcal{R}_n}\xi\Big(\Phi(\gamma g)g^{-1}\begin{pmatrix} n & 0\\ 0 & n\end{pmatrix}\Big).$$

Par définition de Φ, la seconde ligne de $\Phi(\gamma g)g^{-1}(n,0\,;\,0,n)\gamma^{-1}$ (notons $M_{g,\gamma}$ cette matrice) est congrue modulo (N) à celle de la même expression sans Φ : donc $M_{g,\gamma}$ appartient à $\Delta_1^n(N)$. L'ensemble $\Gamma_1(N)\backslash\Delta_1^n(N)$ a le même cardinal que $M_2(\mathbb{Z})_n/\mathrm{SL}_2(\mathbb{Z})$, comme le montre le lemme 3.5 ci-dessous, et puisque lorsque g décrit $\mathcal{R}_n$ les matrices $M_{g,\gamma}$ sont deux à deux non conjuguées par multiplication à gauche par un élément de $\Gamma_1(N)$, $\{M_{g,\gamma}, g\in\mathcal{R}_n\}$ est un ensemble de représentants de $\Gamma_1(N)\backslash\Delta_1^n(N)$. On a donc bien

$$\xi\circ S\circ\big(\Gamma_1(N)\gamma\big) = \sum_{\alpha\in\Gamma_1(N)\backslash\Delta_1^n(N)}\xi(\alpha\cdot\gamma) = T_n\circ\xi\big(\Gamma_1(N)\gamma\big). \qquad \square$$

3.5. Lemme. — *L'application naturelle*

$$\Gamma_1(N)\backslash\Delta_1^n(N)\longrightarrow \mathrm{SL}_2(\mathbb{Z})\backslash M_2(\mathbb{Z})_n$$

est une bijection.

Preuve. — Cette application est clairement injective. Soit $M_1 = (a,b\,;\,c,d)$ un élément de $M_2(\mathbb{Z})_n$, et n' dans $\mathbb{Z}$ tel que $n\cdot n' = 1 \bmod (N)$: la matrice $\overline{M}_2 = (n'\cdot d, -n'\cdot b\,;\,-c,a) \bmod (N)$ appartient à $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Soit $M_2 = (\alpha,\beta\,;\,\gamma,\delta)$ un relèvement dans $\mathrm{SL}_2(\mathbb{Z})$ de $\overline{M}_2$; alors la classe dans $\Gamma_1(N)\backslash\Delta_1^n(N)$ de $M_2\cdot M_1$ s'envoie sur celle de M_1 dans $\mathrm{SL}_2(\mathbb{Z})\backslash M_2(\mathbb{Z})_n$. Donc l'application est surjective. $\square$

La preuve du théorème 3.4 fournit une méthode pour calculer à la main des relèvements (notés Θ_n) des opérateurs de Hecke T_n, si on dispose d'un ensemble de représentants de $M_2(\mathbb{Z})_n/\mathrm{SL}_2(\mathbb{Z})$. Ce que fournit le

3.6. Lemme. — *Pour tout entier $n>0$, l'ensemble*

$$\mathcal{R}_n = \left\{\begin{pmatrix} d & r_d\\ 0 & n/d\end{pmatrix}\in M_2(\mathbb{Z}) \text{ tel que } 0<d\mid n \text{ et } 0\le r_d\le d\right\}$$

est un système de représentants de $M_2(\mathbb{Z})_n/SL_2(\mathbb{Z})$.

Preuve. — Voir [18], lemma 2. $\square$

Application. — On peut donner comme exemple des relèvements des opérateurs de Hecke T_2 et T_3 qui nous intéressent dans le cas des corps cubiques (1.12), comme dans [17], 2.3 :

$$\Theta_2 = (1,0\,;\,0,2) + (2,0\,;\,0,1) + (2,1\,;\,0,1) + (1,0\,;\,1,2),$$

$$\Theta_3 = (1,0\,;\,0,3) + (3,0\,;\,0,1) + (3,1\,;\,0,1) + (1,0\,;\,1,3) + (3,-1\,;\,0,1) + (1,0\,;\,-1,3).$$

Pour pouvoir déterminer l'homologie absolue, donc le noyau de l'opération « bord », on reconnaît l'équivalence de pointes grâce au lemme suivant (voir [1], lemma 3.2) :

3.7. LEMME (Cremona). — *Soient $\alpha = p/q$ et $\beta = r/s$ deux éléments de $\mathbb{P}^1(\mathbb{Q})$ écrits sous forme irréductible. Alors α est conjuguée de β sous l'action de $\Gamma_1(N)$ si et seulement si $q = \epsilon s \bmod (N)$ et $p = \epsilon s \bmod (\mathrm{pgcd}(N,q))$, avec $\epsilon = \pm 1$.*

On peut alors implémenter l'homologie absolue sur machine. Notons :

- $E_1 = \mathrm{Vect}(\text{symboles modulaires})$
  $= \mathrm{Vect}(\{(a,b) \in (\mathbb{Z}/N\mathbb{Z}), (a,b) = (-a,-b)\})$,
- $E_2 = \mathrm{Ker}(\delta)$,
- $E_3 = \mathrm{Vect}(\{(c,1)\ (2 \le c \le (p-1)/2),\ (0,d)\ (1 \le d \le (p-1)/2)\})$,
- $E_4 = \mathrm{Vect}(\{x + x\cdot\sigma, x + x.\tau + x\cdot\tau^2\})$.

On a :

$$H_1(X_1(p)(\mathbb{C}), \text{pointes}\,;\,\mathbb{Z}) \otimes \mathbb{F}_\ell \simeq E_1/E_4,$$

$$H_1(X_1(p)(\mathbb{C}),\,;\,\mathbb{Z}) \otimes \mathbb{F}_\ell \simeq E_2/E_4.$$

On travaille dans E_1 (pour faire agir des opérateurs), on projette le résultat sur E_2 parallèlement à E_3, puis sur un complémentaire de E_4 dans E_2 — ou, lorsqu'on travaille dans l'homologie relative aux pointes — on ne fait que la seconde projection.

4. Explicitation de l'algèbre de Hecke en petit niveau.

4.1. Engendrement de l'algèbre de Hecke par les opérateurs losanges.

Soit C une courbe sur un corps, de genre strictement plus grand que 1. L'application : $\mathrm{Aut}(C) \to \mathrm{Aut}(\mathrm{Jac}(C))$ est injective, d'après [2], th. 1.13. Notons D_p la sous-algèbre de $\mathrm{End}(J_1(p))$ engendrée par les opérateurs losanges. Pour p premier supérieur à 4, le genre de $X_1(p)$ est $g(X_1(p)) = \frac{1}{24}(p-5)(p-7)$ (cela découle facilement de la présentation de Manin, par exemple). Donc si $p \geq 13$, $g(X_1(p)) \geq 2$, et il y a dans D_p un élément d'ordre $\frac{1}{2}(p-1)$.

L'application $\mathbb{Z}[X]/(X^{(p-1)/2}-1) \to D_p$ qui à X associe un générateur du groupe des losanges, est surjective. Notons $\mathbf{Ab}_{\mathbb{Q}} \otimes \mathbb{Q}$ la catégorie des variétés abéliennes sur $\mathbb{Q}$ tensorisée par $\mathbb{Q}$ (les objets restent les variétés abéliennes sur $\mathbb{Q}$, mais on tensorise par $\mathbb{Q}$ les $\mathbb{Z}$-modules des morphismes entre variétés abéliennes). Dans cette catégorie, l'application précédente donne que $J_1(p)$ est un foncteur en modules sur $\prod_{n|(p-1)/2} \mathbb{Q}[\zeta_n]$ (où ζ_n désigne une racine primitive n-ième de l'unité). Remarquons que si $g(X_0(p)) > 0$ le facteur $\mathbb{Q} = \mathbb{Q}[\zeta_1]$ (correspondant au cas «losanges d'action triviale») dans la décomposition de $\mathbb{Q}[X]/(X^{(p-1)/2}-1)$ est dans le support de $\mathrm{End}(J_1(p)) \otimes \mathbb{Q}$, puisqu'il correspond à $\mathrm{End}(J_0(p)) \otimes \mathbb{Q}$. De plus, d'après ce qui précède il existe dans D_p un élément d'ordre maximal, donc si par exemple $\frac{1}{2}(p-1)$ est une puissance d'une nombre premier, le facteur $\mathbb{Q}[\zeta_{(p-1)/2}]$ est également dans le support de $\mathrm{End}(J_1(p)) \otimes \mathbb{Q}$. En niveau 17 et 19, on peut alors montrer par des considérations de dimension que ces deux facteurs du produit ci-dessus constituent tout le support de $\mathrm{End}(J_1(p)) \otimes \mathbb{Q}$, et voir que ce produit de facteurs engendre toute l'algèbre de Hecke sur $\mathbb{Q}$; ce qui rend la description de cette algèbre sur $\mathbb{Z}$ très simple, et donc aussi la vérification des critères 2.7. Explicitons cela.

4.2. Description de l'algèbre de Hecke pour $\Gamma_1(19)$.

La formule du genre énoncée en 4.1 donne que $J_1(19)$ est de dimension 7. Or la dimension sur $\mathbb{Q}$ de $\mathbb{Q}[\zeta_9]$ est 6, et $J_0(19)$ est une courbe elliptique, donc 4.1 implique que $J_1(19)$ est $\mathbb{Q}$-isogène à $J_0(19) \times A_{19}$ dans $\mathbf{Ab}_{\mathbb{Q}} \otimes \mathbb{Q}$, où A_{19} est une variété abélienne simple de dimension 6. Par égalité de dimensions, on a donc $\mathbb{T}_{\Gamma_1(19)} \otimes \mathbb{Q} \simeq \mathbb{Q} \times \mathbb{Q}[\zeta_9]$.

Cela n'implique pas que, sur $\mathbb{Z}$, l'algèbre de Hecke soit égale à D_{19} (isomorphe à $\mathbb{Z}[X]/(X-1) \cdot \Phi_9(X)$, où Φ_n désigne dorénavant le n-ième

polynôme cyclotomique) : tout au plus cette sous-algèbre est-elle d'indice fini dans $\mathbb{T}_{\Gamma_1(19)}$. Cependant les composantes irréductibles de $\mathrm{Spec}(D_{19})$ définies par $(X-1)$ et $(\Phi_9(X))$ ne s'intersectent qu'au-dessus de 3, donc sur $\mathrm{Spec}(\mathbb{Z}[1/3])$, D_{19} est intégralement clos et l'on a :

$$\begin{aligned}\mathbb{T}_{\Gamma_1(19)} \otimes \mathbb{Z}[1/3] &\simeq D_{19} \otimes \mathbb{Z}[1/3] \\ &\simeq \mathbb{Z}[1/3][X]/(X-1) \times \mathbb{Z}[1/3][X]/(X^6+X^3+1),\end{aligned}$$

et ces isomorphismes valent en particulier dans la fibre en 2 qui nous intéresse.

Vérifions alors les critères de 1.12. Notons d'abord que les calculs explicités dans la partie 5 montrent, en supposant $(*)_{19}$ vraie (1.1), que $J_1(19)$ est de rang nul sur $\mathbb{Q}$, donc qu'on peut prendre l'opérateur t_1 de 1.10 égal à 1. Pour exprimer les opérateurs de Hecke T_2, T_3 (et T_7), on dispose des tables de [13] :

- sur $\mathbb{Z}[1/3][X]/(X-1)$, on a $\langle 2\rangle = 1$, $T_2 = 0$, $T_3 = -2$, et $T_7 = -1$;
- sur $\mathbb{Z}[1/3][X]/(\Phi_9(X))$, on a $\langle 2\rangle = X$,
  $T_2 = (-2+X+X^8).(1+X) \equiv 1+X+X^5 \bmod (2)$,
  $T_3 = (X+X^8).(1+X^4) \equiv X+X^2+X^3 \bmod (2)$, et
  $T_7 = (-2+(X+X^8)+(X+X^8)^2)\cdot(1+X^6)$
  $\equiv X+X^2+X^4+X^5 \bmod (2)$.

On choisit a_7 comme « t_2 » annulant les μ_2 (voir 1.8 et 1.10), valant $X+X^2+X^4+X^5$ dans $\mathbb{F}_2[X]/(X^6+X^3+1)$, et 1 dans $\mathbb{F}_2[X]/(X-1)$ (les calculs montrent que a_3 ne convient pas ici). On a donc, dans $\mathbb{F}_2[X]/(X^6+X^3+1)$,

$$\begin{aligned}
a_7\cdot T_1 &\equiv X^5+X^4+X^2+X, & a_7\cdot T_2 &\equiv X^3+X+1,\\
a_7\cdot T_3 &\equiv X^5, & a_7\cdot\langle 2\rangle &\equiv X^5+X^2+1,\\
a_7\cdot\langle 3\rangle &\equiv X^3+X^2, & a_7\cdot\langle 4\rangle &\equiv X+1,\\
a_7\cdot\langle 5\rangle &\equiv X^5+X^3+1, & a_7\cdot\langle 6\rangle &\equiv X^4+X^3,\\
a_7\cdot\langle 7\rangle &\equiv X^5+X^4, & a_7\cdot\langle 8\rangle &\equiv X^2+X,\\
a_7\cdot\langle 9\rangle &\equiv X^4+X^3+X+1. & &
\end{aligned}$$

On vérifie alors l'indépendance linéaire des éléments des familles de la proposition (1.12) (elles sont même toutes $\mathbb{F}_2$-libres dans le seul facteur $\mathbb{F}_2[X]/(X^6+X^3+1)$, sauf $(a_7.\langle 1\rangle, a_7\cdot\langle 8\rangle, a_7\cdot\langle 7\rangle)$ qui y est égal à $(a_7\cdot 1, a_7\cdot X^3, a_7\cdot X^6)$: on vérifie cependant que cette famille est libre dans $\mathbb{F}_2[X]/(X^6+X^3+1)\times\mathbb{F}_2[X]/(X-1)$). On a donc exclu 19 de $S(3)$.

4.3. Description de l'algèbre de Hecke pour $\Gamma_1(17)$.

On va tenter de procéder de même avec 17. De même que pour $\Gamma_1(19)$, on voit que $J_1(17)$ est de dimension 5, que $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = 4$, et que comme $J_0(17)$ est de dimension 1, $J_1(17) \simeq J_0(17) \times A_{17}$ dans $\mathbf{Ab}_{\mathbb{Q}} \otimes \mathbb{Q}$, ($A_{17}$ variété abélienne simple de dimension 4); donc $\mathbb{T}_{\Gamma_1(17)} \otimes \mathbb{Q} \simeq \mathbb{Q} \times \mathbb{Q}[\zeta_8]$. Sur $\mathbb{Z}$, $\mathbb{T}_{\Gamma_1(17)}$ (qui est un $\mathbb{Z}$-module de type fini) est égal soit à

$$D_{17} \simeq \mathbb{Z}[X]/(X-1)\Phi_4(X) (= \mathbb{Z}[X]/(X-1)(X^4+1)),$$

soit à son normalisé $\overline{D}_{17}$ dans $D_{17} \otimes \mathbb{Q}$, qui est $\mathbb{Z}[X]/(X-1) \times \mathbb{Z}[X]/(X^4+1)$ (en effet, l'indice de D_{17} dans $\overline{D}_{17}$ est 2). Donc $\mathbb{T}_{\Gamma_1(17)} \otimes \mathbb{F}_2$ est égal soit à $D_{17} \otimes \mathbb{F}_2$ ($\simeq \mathbb{F}_2[X]/(X+1)^5$), soit à

$$\overline{D}_{17} \otimes \mathbb{F}_2 \quad \left(\simeq \mathbb{F}_2[X]/(X+1) \times \mathbb{F}_2[X]/(X+1)^4\right).$$

Pour déterminer $\mathbb{T}_{\Gamma_1(17)}$, il suffit de savoir si les coefficients des formes propres sont les mêmes jusqu'à l'indice $(2g-2)+1 = 9$ (g désignant le genre de la courbe modulaire; $(2g-2)$ est en effet le degré du diviseur canonique). Il est donc suffisant de savoir si, pour chaque paire de formes propres, les coefficients de ces formes d'indice premier $p \leq 7$ sont égaux modulo 2 : la réponse est positive, comme un calcul direct avec les tables de [13] ou [29] le montre [(1)]. Mais on peut aussi remarquer que cela découle de ce que les losanges agissent trivialement modulo (2). Soit en effet f la différence de deux formes nouvelles de $S_2(\Gamma_1(17))_{\mathbb{F}_2}$. Le fait que ces deux formes modulaires soient normalisées entraîne que f s'annule au moins en une pointe de $X_1(17)_{\mathbb{F}_2}$ au-dessus de $\infty_{\mathbb{F}_2} \in X_0(17)_{\mathbb{F}_2}$; donc elle s'annule en toutes, puisque toutes sont conjuguées sous les losanges. De plus l'involution d'Atkin-Lehner w agit trivialement en caractéristique 2, donc $w(f) = f$ s'annule aussi en les huit pointes de $X_1(17)_{\mathbb{F}_2}$ au-dessus de $0_{\mathbb{F}_2} \in X_0(17)_{\mathbb{F}_2}$: f a strictement plus de zéros que le degré du diviseur canonique, donc elle est nulle. On déduit de tout cela que $\mathbb{T}_{\Gamma_1(17)} = D_{17}$.

---

(1) L'anneau des entiers de $\mathbb{Q}[\zeta_8]$ est totalement ramifié en 2, et $\pi = (\zeta_8 - 1)$ est une uniformisante de $\mathbb{Z}[\zeta_8]_{(2)}$; soit v_π la valuation discrète de cet anneau normalisée par $v_\pi(\pi) = 1$. Les tables de [13] ou [29] donnent que les expressions de T_2, T_3, T_5 et T_7 dans $\mathbb{Q}[\zeta_1]$ sont $\lambda_2 = -1$, $\lambda_3 = 0$, $\lambda_5 = -2$ et $\lambda_7 = 4$ respectivement, et dans $\mathbb{Q}[\zeta_8]$,

$$\lambda'_2 = \frac{1}{2}(-2 + \zeta_8 + \zeta_8^7)(1 + \zeta_8^6), \qquad \lambda'_3 = -(\zeta_8 + \zeta_8^7)(1 + \zeta_8),$$

$$\lambda'_5 = (1 + \zeta_8 + \zeta_8^7)(1 + \zeta_8^5), \qquad \lambda'_7 = (\zeta_8 + \zeta_8^7).(1 + \zeta_8^3).$$

Il est clair que $v_\pi(\lambda'_3) > 0$, $v_\pi(\lambda'_5) > 0$ et $v_\pi(\lambda'_7) > 0$. Puis $v_\pi(1 + \zeta_8^6) = v_\pi(1 - i) = 2$, et $v_\pi(-2 + \zeta_8 + \zeta_8^7) = v_\pi(\zeta_8^7(\zeta_8^2 - 2.\zeta_8 + 1)) = v_\pi((\zeta_8 - 1)^2) = 2$, donc $v_\pi(\lambda'_2) = 0$.

Pour vérifier les critères de Kamienny, exprimons alors les opérateurs de Hecke comme des éléments de $\mathbb{Z}[X]/(X-1)(X^4+1)$ (on connaît par [13] leur image dans $\mathbb{Z}[X]/(X-1) \times \mathbb{Z}[X]/(X^4+1)$) :

$$T_2 = -X^3 + X^2 - 1, \quad T_3 = X^4 + X^3 - X^2 - X,$$
$$\langle 2 \rangle = X^4 - X^2 + 1, \quad \langle 3 \rangle = X,$$
$$\langle 4 \rangle = X^4, \quad \langle 5 \rangle = X^4 - X + 1,$$
$$\langle 6 \rangle = X^4 - X^3 + 1, \quad \langle 7 \rangle = X^3,$$
$$\langle 8 \rangle = X^2.$$

Comme dans le cas de $\Gamma_1(19)$, on montre dans la partie 5 (sous l'hypothèse $(*)_{17}$) que $J_1(17)$ est de rang nul sur $\mathbb{Q}$. Les critères de Kamienny à vérifier sont donc l'indépendance linéaire des familles (t_2T_1, t_2T_2, t_2T_3), *etc.*, avec t_2 un annulateur de μ_2 (par exemple a_3 (1.8)). Or si on vérifie facilement que toutes les familles *non multipliées par* t_2 sont bien $\mathbb{F}_2$-linéairement indépendantes, on voit aussi que la multiplication par $\langle 4 \rangle = X^4 \equiv 1 + (X-1)^4 \bmod (2)$, par exemple, vaut l'identité sur tout élément non-inversible de $\mathbb{T}_{\Gamma_1(17)} \otimes \mathbb{F}_2 \simeq \mathbb{F}_2[X]/(X-1)^5$: aucun critère de Kamienny « complet » ne sera donc vérifié (c'est-à-dire l'indépendance linéaire de *toutes* les familles de 1.10 pour $p = 17$ et $d = 3$, avec un élément t_2 non trivial). On peut cependant dire de tout ça quelque chose.

D'abord, on calcule quels sont les triplets comme en 1.12, avec $t_1 = 1$ et $t_2 = a_3$, qui ne sont pas de rang 3. Supposons que le point $j^{(d)}$, construit dans la section 1.5 à partir d'une courbe elliptique ayant un point de 17-torsion sur un corps cubique, corresponde à un de ces « mauvais triplets ». Si $j^{(d)}$ n'est pas d'image nulle par le morphisme qui lui est associé $(f'_{P_0} : X_1(17) \to J_1(17),\ Q \mapsto (Q - P_0))$, il ne peut s'envoyer que sur un générateur d'un μ_2 de $J_1(17)(\mathbb{Z}_{(2)})$ selon 1.7 (et chacun de ces générateurs ne peut avoir qu'un tel $j^{(d)}$ dans son image réciproque, puisque f'_{P_0} est une immersion formelle en $j^{(d)}(\mathbb{F}_\ell) = P_0(\mathbb{F}_\ell)$). La 2-torsion étant de rang 10 sur $J_1(17)[2](\overline{\mathbb{Q}})$, il y a au plus $(2^{10} - 1) = 1023$ images possibles pour $j^{(d)}$; en fait, en utilisant la formule de Lefschetz et l'expression des polynômes minimaux d'opérateurs de Hecke, puis en éliminant la 2-torsion engendrant des $\mathbb{Z}/2\mathbb{Z}$ qu'on trouve dans l'intersection du sous-groupe de Shimura avec le sous-groupe cuspidal, on a calculé qu'il y avait au plus 7 points non triviaux d'ordre 2 dans $J_1(17)(\mathbb{Q})$. Chaque triplet des 8 pointes au-dessus de $\infty \in X_0(p)$ correspondant à un « mauvais triplet de 1.12 » donne lieu à un morphisme f'_{P_0}, ce qui fait au pire $(8 + 8 \times 3 + 8 \times 3) \times 7 = 392$ éléments de $Y_1(17)^{(3)}(\mathbb{Q})$, soit au plus ce nombre de classes d'isomorphismes de

triplets (K, E, P) avec K un corps cubique, E une courbe elliptique sur K, $P \in E(K)[17]$ (un tel triplet étant dit isomorphe à un second (K', E', P') s'il y a un isomorphisme de K dans K' tel que (E, P) soit isomorphe au changement de base de (E', P') par K). Mais on ne se préoccupe pas du générateur des groupes de 17-torsion dans la définition d'isomorphisme du théorème 1.4 : on peut donc diviser le nombre précédent par 8, d'où le résultat en 1.4. (En effet, les huit triplets $(E, K, \pm n \cdot P)$ comme ci-dessus avec $n \in \mathbb{F}_{17}^*$ donnent huit points distincts de $X_1(17)^{(3)}(\mathbb{Q})$: on aurait sinon un morphisme non trivial du groupe d'automorphismes de K dans $\mathbb{F}_{17}^*/(\pm 1)$.)

5. Résultats de calcul.

Pour minorer la dimension du quotient d'enroulement en niveau 17, 19, 23, 29, 31 et 37, on a calculé sur machine le rang de familles d'éléments de $\mathbb{T}_{\Gamma_1(N)} \cdot e \otimes \mathbb{F}_2$, explicitement $F = \{\tau_i \cdot A_q \cdot \{0, \infty\}\}$, les τ_i étant T_2, T_3, T_7 et les opérateurs losanges, q prenant les valeurs 2, 3 et 7 (les deux premiers étant déjà implémentés pour les critères de Kamienny, le troisième parce que A_7 est le premier dont on est sûr qu'il soit inversible sur $\mathbb{Q}$ (voir [4])). On a en effet les implications suivantes :

$$\begin{aligned}
&\Big(\sum \lambda_i \tau_i \cdot e = 0 \in \mathbb{T}_{\Gamma_1(N)} \cdot e \subseteq H_1(X_1(p)(\mathbb{C}) ; \mathbb{Q}), \operatorname{pgcd}(\lambda_i) = 1\Big) \\
&\quad \Rightarrow \Big(\sum \lambda_i \tau_i \cdot A_\ell \cdot e = 0 \in H_1(X_1(p)(\mathbb{C}) ; \mathbb{Z}),\ \operatorname{pgcd}(\lambda_i) = 1\Big) \\
&\quad \Rightarrow \Big(\sum \lambda_i \tau_i . A_\ell . \{0, \infty\} = 0 \in H_1(X_1(p)(\mathbb{C}), \text{pointes} ; \mathbb{Z}),\ \operatorname{pgcd}(\lambda_i) = 1\Big).
\end{aligned}$$

En explicitant par [13] ou [29] la décomposition en facteurs simples sur $\mathbb{Q}$ des $J_1(p)$ pour les niveaux ci-dessus, on obtient les résultats suivants (le signe $\sim$ signifiant « est isogène à ») :

- $J_1(17) \sim J_0(17) \times A_1$, $J_0(17)$ et A_1 variétés simples sur $\mathbb{Q}$ de dimensions respectives 1 et 4, et $\operatorname{rang}_{\mathbb{F}_2}(F) = 4$;
- $J_1(19) \sim J_0(19) \times A_1$, $J_0(19)$ et A_1 variétés simples sur $\mathbb{Q}$ de dimensions respectives 1 et 6, et $\operatorname{rang}_{\mathbb{F}_2}(F) = 7$;
- $J_1(23) \sim J_0(23) \times A_1$, $J_0(23)$ et A_1 variétés simples sur $\mathbb{Q}$, de dimensions 2 et 10, et $\operatorname{rang}_{\mathbb{F}_2}(F) = 12$;
- $J_1(29) \sim J_0(29) \times A_1 \times A_2 \times A_3$, $J_0(29), \ldots, A_3$ variétés simples sur $\mathbb{Q}$ de dimensions 2, 2, 6, 12, et $\operatorname{rang}_{\mathbb{F}_2}(F) = 22$;

• $J_1(31) \sim J_0(31) \times A_1 \times A_2 \times A_3$, $J_0(31), \ldots, A_3$ variétés simples sur $\mathbb{Q}$ de dimensions 2, 4, 4, 16, et $\text{rang}_{\mathbb{F}_2}(F) = 24$;

• $J_1(37) \sim A_1 \times A_2 \times A_3 \times \cdots \times A_8$ ($J_0(37) \sim A_1 \times A_2$), $A_1, \ldots, A_8$ variétés simples sur $\mathbb{Q}$ de dimensions 1, 1, 2, 2, 4, 6, 6, 18 et $\text{rang}_{\mathbb{F}_2}(F) = 39$.

Enfin,

• $J_1(43) \sim A_1 \times A_2 \times A_3 \times \cdots \times A_7$ ($J_0(43) \sim A_1 \times A_4$), $A_1 \ldots A_7$ variétés simples sur $\mathbb{Q}$ de dimensions 1, 6, 6, 2, 36, 2, 4.

En tenant compte du fait que le quotient d'enroulement des $J_0(p)$ n'est pas nul (et donc égal à $J_0(p)$ tout entier lorsque celle-la est simple), on en déduit que $J_1(p)$ est de rang nul sur $\mathbb{Q}$ pour les niveaux 17, 19, 23, 29 et 31. Pour le niveau 37, on voit que le quotient d'enroulement est de dimension 39. Pour le niveau 43, on a pu travailler en caractéristique 3 (voir 1.11); le lemme 1.9 nous a permis de déterminer que seuls A_1 et éventuellement A_6 sont des facteurs simples du quotient d'enroulement de $J_1(43)$. Dans les deux cas : $p = 37$ et $p = 43$, on a déterminé un élément de l'orthogonal de l'idéal d'enroulement à partir de l'opérateur T_2, grâce au lemme 1.9 ($T_2^2 + 2T_2$ pour $p = 37$ et $T_2^2 + T_2 - 2$ pour $p = 43$). On a construit ainsi pour chaque niveau un opérateur t_1, avec les notations de 1.10; pour t_2, on choisit a_3 (1.8), sauf en niveau 19 où il a fallu employer a_7, et en niveau 43, où le fait de n'être pas en caractéristique 2 a permis de prendre $t_2 = 1$ (1.10).

On a alors vérifié par ordinateur les « critères de Kamienny » (1.12) au cas par cas, pour les niveaux 23, 29, 31, 37 et 43 (ainsi que retrouvé nos calculs « à la main » dans les cas de 17 et 19).

BIBLIOGRAPHIE

[1] J.E. CREMONA, Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction, Math. Proc. Camb. Phil. Soc., 111 (1992), 199–218.

[2] P. DELIGNE, D. MUMFORD, On the Irreducibility of the Space of Curves of Given Genus, Publ. Math. IHES, 36 (1969), 75–110.

[3] F. DIAMOND, J. IM, Modular forms and modular curves, Canadian Math. Soc. Conf. Proc., 17 (1995), 39–133.

[4] V.G. DRINFELD, Two theorems on modular curves, Funktsional Anal. i Prilozhen, 7, n° 2 (1973), 82–84 (en russe); Functional Anal. Appl., 7, n° 2 (1973), 155–156 (en anglais).

[5] B.H. GROSS, A tameness criterion for Galois representations associated to modular forms (mod (p)), Duke Math. J., 61 (1990), 445–517.

[6] A. GROTHENDIECK, M. RAYNAUD, D.S. RIM, Séminaire de géométrie algébrique 7–I, Lecture Notes in Math., 288 (1972).

[7] S. KAMIENNY, Torsion points on elliptic curves and q–coefficients of modular forms, Invent. Math., 109 (1992), 221–229.

[8] S. KAMIENNY, Some remarks on torsion in elliptic curves, Comm. in Algebra, 23 (6) (1995), 2167–2169.

[9] S. KAMIENNY, B. MAZUR, Rational torsion of prime order in elliptic curves over number fields, Astérisque, 228 (1995), 81–100.

[10] K. KATO, Euler systems, Iwasawa theory, and Selmer groups, à paraître.

[11] N.M. KATZ, B. MAZUR, Arithmetic moduli of elliptic curves, Annals of Math. Studies, Princeton University Press, 108 (1985).

[12] M.A. KENKU, F. MOMOSE, Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J., 109 (1988), 125–149.

[13] J.–C. LARIO, J. QUER, Table of some Hecke operators' eigenvalues, non publiée.

[14] Y. MANIN, Parabolic points and zeta function of modular curves, Math. USSR Izvestija, 6 (1972), 19–64.

[15] B. MAZUR, Modular curves and the Eisenstein ideal, Pub. Math. I.H.E.S., 47 (1977), 33–186.

[16] B. MAZUR, Rational Isogenies of Prime Degree, Invent. Math., 44 (1978), 129–162.

[17] L. MEREL, Opérateurs de Hecke pour $\Gamma_0(N)$ et fractions continues, Annales Institut Fourier, 41–1 (1991), 519–537.

[18] L. MEREL, Universal Fourier expansions of modular forms, in On Artin's conjecture for odd 2–dimensional representations, Lecture Notes Math., 1585, Springer-Verlag (1994), 59–94.

[19] L. MEREL, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Invent. Math., 124 (1996), 437–449.

[20] F. MOMOSE, p–Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J., 96 (1984), 139–165.

[21] J. OESTERLÉ, Torsion des courbes elliptiques sur les corps de nombres, non publié.

[22] P. PARENT, Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres, J. reine ang. Math., 506 (1999), 85–116.

[23] A. PETHÖ, Th. WEIS, H. ZIMMER, Torsion of elliptic curves with integral j-invariant over general cubic number fields, Internat. J. Alg. and Comp., 7, 3 (1997), 353–413.

[24] M. RAYNAUD, Schémas en groupes de type $(p,\ldots,p)$, Bull. Soc. Math. France, 102 (974), 241–280.

[25] K. RUBIN, Euler systems and modular elliptic curves, in Galois representations in arithmetic algebraic geometry (Durham 1996), London Math. Soc. Lecture Note Ser., 254 (1998), Cambridge University Press, Cambridge, 351–367.

[26] A. SCHOLL, An introduction to Kato's Euler systems, in Galois representations in arithmetic algebraic geometry (Durham 1996), London Math. Soc. Lecture Note Ser., 254 (1998), Cambridge University Press, Cambridge , 379–460.

[27] J.-P. SERRE, Lectures on the Mordell–Weil Theorem (third ed.), Aspects of Mathematics, Vieweg (1997).

[28] G. SHIMURA, Introduction to the Arithmetic Theory of Automorphic Functions, Princeton University Press, 1971.

[29] W. STEIN, disponible sur la toile en http://shimura.math.berkeley.edu/~was/Tables/index.html.

Manuscrit reçu le 4 juin 1999,
accepté le 15 octobre 1999.

Pierre PARENT,
Université de Rennes I
Campus de Beaulieu
IRMAR
35 042 Rennes Cedex (France).
parent@maths.univ–rennes1.fr