Journal de Théorie des Nombres
de Bordeaux **7** *(1995), 283–306*

Jacobiennes de certaines courbes de genre 2 : torsion et simplicité.

par Franck LEPREVOST

Introduction :

Nous construisons ici, pour $l = 21, 22, 23, 25, 26, 27$ et 29 une courbe de genre 2 définie sur $\mathbf{Q}$, dont la jacobienne possède un point d'ordre l rationnel sur $\mathbf{Q}$. La méthode employée permet, pour $l = 24$, de construire deux telles courbes non $\overline{\mathbf{Q}}$-isomorphes. Dans un même esprit, nous construisons une famille à un paramètre de courbes de genre 2, définies sur $\mathbf{Q}$, dont la jacobienne possède un sous-groupe isomorphe à $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z}$.
Nous examinons dans un premier temps les courbes modulaires de genre 2 ; $X_1(13)$, $X_1(18)$ et $X_1(16)$. Les jacobiennes de ces courbes possèdent respectivement un point rationnel d'ordre 19, 21 et 10. Cette première section contient également l'énoncé de nos résultats.
L'étude de ces courbes particulières, principalement $X_1(13)$ et $X_1(18)$, suggère une méthode pour obtenir des courbes de genre 2, définies sur $\mathbf{Q}$, dont la jacobienne possède un sous-groupe de torsion rationnel non trivial. Cette méthode est décrite dans le deuxième paragraphe.
Dans le dernier paragraphe, nous donnons un critère d'absolue simplicité de la jacobienne d'une courbe de genre 2 définie sur $\mathbf{Q}$. Nous montrons ainsi que certaines des courbes obtenues dans le deuxième paragraphe ont des jacobiennes absolument simples.
Ce travail, annoncé pour l'essentiel dans [3], étend des résultats décrits dans [2].
Remerciements. Je tiens à exprimer ma reconnaissance à Jean-François Mestre pour son aide lors de ce travail.

Table des matières

Manuscrit reçu le 4 octobre 1993.
Manuscrit reçu le 19 novembre 1993, version corrigée le 28 avril 1994.

1. L'exemple de certaines courbes modulaires.

1.1. Les courbes modulaires $X_1(13)$, $X_1(18)$ et $X_1(16)$. Nous examinons dans cette section les courbes modulaires $X_1(N)$ de genre 2. Tel est le cas si et seulement si $N = 13, 16$ ou 18 (*cf.* [5] p. 226). Les équations que nous donnons ici de ces courbes se déduisent aisément de celles données dans [6] (théorème 1 p. 638).
Considérons en premier lieu la courbe modulaire $X_1(13)$. Une équation de cette courbe est :

$$y^2 = f_{19}(x) = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1.$$

On constate que

$$f_{19}(x) = A^2(x) + 4x(x-1) = B^2(x) - 4x^4(x-1) = C^2(x) - 4x(x-1)^2,$$

où

$$\begin{aligned} A(x) &= -x^3 + x^2 + 1, \\ B(x) &= x^3 + x^2 - 2x + 1, \\ C(x) &= x^3 - x^2 + 1. \end{aligned}$$

Soient $\varphi_1(x,y) = y - A(x)$, $\varphi_2(x,y) = y - B(x)$ et $\varphi_3(x,y) = y - C(x)$, et notons

$$\begin{aligned} D_0 &= (0, A(0)) - (+\infty) = (0,1) - (+\infty), \\ D_1 &= (1, A(1)) - (+\infty) = (1,1) - (+\infty), \\ D_\infty &= (-\infty) - (+\infty), \end{aligned}$$

D_0, D_1, D_∞ sont des diviseurs rationnels sur la courbe.
Un rapide calcul montre que

$$\begin{pmatrix} (\varphi_1) \\ (\varphi_2) \\ (\varphi_3) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 4 & 1 & -3 \\ 1 & 2 & -3 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix}$$

Par suite

$$\begin{pmatrix} (\varphi_3\varphi_1^3) \\ (\varphi_2/\varphi_3) \\ (\varphi_3) \end{pmatrix} = \begin{pmatrix} 4 & 5 & 0 \\ 3 & -1 & 0 \\ 1 & 2 & -3 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix}$$

et donc la classe du diviseur D_0 (par exemple) est d'exposant 19. En effet,

$$\left(\frac{{\varphi_1}^3{\varphi_2}^5}{{\varphi_3}^4}\right) = 19D_0.$$

Enfin, le genre de $X_1(13)$ étant non nul, il est clair que le diviseur D_0 définit un élément rationnel d'ordre 19 de la jacobienne de $X_1(13)$.

Considérons maintenant la courbe modulaire $X_1(18)$, dont une équation est :

$$y^2 = f_{21,1}(x) = x^6 - 4x^5 + 10x^4 - 10x^3 + 5x^2 - 2x + 1.$$

On constate que

$$f_{21,1}(x) = A^2(x) - 4x^2(x-1)^3 = B^2(x) + 4x^3(x-1) = C^2(x) + 8x^2(x-1)^2,$$

où

$$\begin{aligned} A(x) &= x^3 - x + 1, \\ B(x) &= -x^3 + 2x^2 - x + 1, \\ C(x) &= -x^3 + 2x^2 + x - 1. \end{aligned}$$

Un calcul analogue au précédent montre que la classe du diviseur $D_\infty = (-\infty) - (+\infty)$ est d'ordre 21.

Considérons enfin la courbe modulaire $X_1(16)$, dont une équation est :

$$y^2 = f_{2,10}(x) = (x-1)(x+1)(x^2+1)(x^2+2x-1).$$

On constate que

$$f_{2,10}(x) = A^2(x) - 4x^2 = B^2(x) + 4x(x-1)(x+1),$$

où

$$\begin{aligned} A(x) &= x^3 + x^2 - x + 1, \\ B(x) &= (x-1)(x+1)^2. \end{aligned}$$

Comme précédemment, il est facile de voir que la classe de $D = (0,1) + (-\infty) - 2(+\infty)$ est d'ordre 2 et que celle de $(-\infty) - (+\infty)$ est d'ordre 5.

Nous avons ainsi montré que la jacobienne de la courbe modulaire $X_1(13)$ (resp. $X_1(18)$, resp. $X_1(16)$) possède un point rationnel d'ordre 19 (resp. 21, resp. 10) ; en fait (*cf.* [5] p. 226), le groupe de torsion de la jacobienne de $X_1(13)$ (resp. $X_1(18)$, resp. $X_1(16)$) est isomorphe à $\mathbf{Z}/19\mathbf{Z}$ (resp. $\mathbf{Z}/21\mathbf{Z}$, resp. $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/10\mathbf{Z}$).

1.2. Les résultats.

THÉORÈME 1.2.1. *Pour $l = 21, 22, 23, 25, 26, 27$ et 29, il existe une courbe, C_l, définie sur $\boldsymbol{Q}$, de genre 2 d'équation*

$$y^2 = f_l(x)$$

et dont la jacobienne possède un point rationnel d'ordre l. Pour $l = 24$, il existe 2 courbes définies sur $\boldsymbol{Q}$ et de genre 2, $C_{l,1}$ et $C_{l,2}$, non $\overline{\boldsymbol{Q}}$-isomorphes, d'équations respectives

$$y^2 = f_{l,1}(x) \text{ et } y^2 = f_{l,2}(x),$$

et dont la jacobienne possède un point rationnel d'ordre l.

Plus précisément :

$$\begin{aligned}
f_{21}(x) &= 4x^6 - 12x^5 + 13x^4 - 6x^3 + 3x^2 - 2x + 1, \\
f_{22}(x) &= (2x^2 - 2x + 1)(2x^4 - 2x^3 + x^2 - 4x + 4), \\
f_{23}(x) &= x^6 - 10x^5 + 33x^4 - 36x^3 + 28x^2 - 16x + 4, \\
f_{24,1}(x) &= (2x^2 - 2x - 1)(2x^4 - 10x^3 + 7x^2 + 4x - 4) \\
f_{24,2}(x) &= (x^2 - x + 1)(x^4 - 3x^3 + 8x^2 - 3x + 1), \\
f_{25}(x) &= 36x^6 - 156x^5 + 241x^4 - 192x^3 + 102x^2 - 36x + 9, \\
f_{26}(x) &= (6x^2 - 6x + 1)(6x^4 - 30x^3 + 49x^2 - 20x + 4), \\
f_{27}(x) &= (2x^3 - 15x^2 + 12x - 3)(2x^3 - 15x^2 - 3), \\
f_{29}(x) &= (2x - 1)(2x^5 - x^4 - 4x^2 + 8x - 4)
\end{aligned}$$

Par ailleurs,

THÉORÈME 1.2.2. *Il existe une famille à un paramètre de courbes de genre 2 et définies sur $\boldsymbol{Q}$, dont la jacobienne possède un sous-groupe isomorphe à $\boldsymbol{Z}/3\boldsymbol{Z} \times \boldsymbol{Z}/9\boldsymbol{Z}$.*

COROLLAIRE 1.2.3. *Il existe une infinité de courbes de genre 2, définies sur $\boldsymbol{Q}$, deux à deux non $\overline{\boldsymbol{Q}}$-isomorphes, dont la jacobienne possède un sous-groupe isomorphe à $\boldsymbol{Z}/3\boldsymbol{Z} \times \boldsymbol{Z}/9\boldsymbol{Z}$.*

Plus précisément, il s'agit de la courbe C_t, d'équation

$$\begin{aligned}
y^2 &= x^6 + 6(t-1)x^5 + 3(t-1)(3t-5)x^4 - (18t^2 - 34t + 18)x^3 \\
&\quad +3(t-1)(5t-3)x^2 - 6t(t-1)x + t^2.
\end{aligned}$$

2. La méthode

Les formes que revêtent f_{19} et $f_{21,1}$ suggèrent la méthode suivante. Elle consiste à partir d'une équation :

$$f(x) = P_i^2(x) + \lambda_i x^{\alpha_i}(x-1)^{\beta_i},$$

où $i = 1, 2$, $P_i \in \mathbf{Q}[x]$ de degré 3, $(\alpha_i, \beta_i) \in \mathbf{N}^2$, avec $\alpha_i + \beta_i \leq 5$ et $\lambda_i \in \mathbf{Q}^*$ de sorte que la courbe E d'équation

$$y^2 = f(x),$$

soit de genre 2. On suppose de plus que $P_2(0) = \pm P_1(0)$ et $P_2(1) = \pm P_1(1)$.

Notons D_0, D_1, D_∞ les diviseurs rationnels sur la courbe E :

$$\begin{array}{rcl} D_0 & = & (0, P_1(0)) - (+\infty), \\ D_1 & = & (1, P_1(1)) - (+\infty), \\ D_\infty & = & (-\infty) - (+\infty). \end{array}$$

On essaie alors de trouver une troisième écriture pour $f(x)$:

$$f(x) = P_3^2(x) + \lambda_3 x^{\alpha_3}(x-1)^{\beta_3},$$

du même type que les précédentes, et compatible avec les deux conditions suivantes :

D'une part, le genre de E est 2. D'autre part, soient, pour $i = 1, 2, 3$, $\varphi_i(x, y)$ des fonctions, construites naturellement à partir des fonctions $y - P_i(x)$, telles que

$$\begin{pmatrix} (\varphi_1) \\ (\varphi_2) \\ (\varphi_3) \end{pmatrix} = \begin{pmatrix} K & L & M \\ N & O & P \\ Q & R & S \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix}$$

On exige que le déterminant de la matrice

$$\begin{pmatrix} K & L & M \\ N & O & P \\ Q & R & S \end{pmatrix}$$

soit $\neq 0$. L'ordre de la classe des diviseurs D_0, D_1 et D_∞ sera un diviseur de ce déterminant.

Nous utilisons cette méthode ci-dessous pour obtenir les courbes décrites dans les théorèmes **1.2.1** et **1.2.2**. L'étude de la simplicité des jacobiennes de ces courbes est faite dans le paragraphe **3.2**.

2.1. $l = 21$. Soient λ et μ des éléments de $\mathbf{Q}^*$, et A et B des éléments de $\mathbf{Q}[x]$ de degré 3 tels que

$$f(x) = A^2(x) + \lambda x^2(x-1) = B^2(x) + \mu x(x-1)^2$$

soit sans racines multiples. Notons E la courbe de genre 2 d'équation

$$y^2 = f(x).$$

On a l'équation :

$$(B-A)(B+A) = x(x-1)[\lambda x - \mu(x-1)].$$

Une solution de cette équation, avec $d^0(A) = d^0(B) = 3$, est :

$$\begin{aligned} A(x) &= \frac{x(x-1)(\lambda x - \mu(x-1))}{2} - \frac{1}{2}, \\ B(x) &= \frac{x(x-1)(\lambda x - \mu(x-1))}{2} + \frac{1}{2}, \end{aligned}$$

Cherchons à écrire $f(x)$ sous la forme $f(x) = C^2(x) + \xi x^2(x-1)^2$, où $C \in \mathbf{Q}[x]$ est de degré 3 et $\xi \in \mathbf{Q}^*$. Cela impose

$$(C-A)(C+A) = x^2(x-1)[\lambda - \xi(x-1)]. \tag{1}$$

Notons que x ne peut diviser $C-A$ et $C+A$, car alors x diviserait A et f ne serait pas sans racines multiples.
La solution de (1) ne menant pas à une courbe singulière est

$$\begin{cases} A(x) = \frac{x-1}{2u} - \frac{ux^2(\lambda - \xi(x-1))}{2} \\ C(x) = \frac{x-1}{2u} + \frac{ux^2(\lambda - \xi(x-1))}{2} \end{cases}$$

où $u \in \mathbf{Q}^*$.
Les conditions de compatibilité de cette expression pour A avec celle obtenue en fonction de λ, μ sont

$$\begin{cases} 1-u = 0 \\ -u\beta - 1 = 0 \\ u(u\lambda + u\xi + 2\beta - \lambda) = 0 \\ u(-u\xi + \lambda - \beta) = 0 \end{cases}$$

soit

$$\begin{cases} u = 1 \\ \xi = 2 \\ \beta = -1 \\ \lambda = -1 \end{cases}$$

D'où

$$f(x) = \frac{4x^6 - 12x^5 + 13x^4 - 6x^3 + 3x^2 - 2x + 1}{4},$$

et l'on a, après changement de y en $\frac{y}{2}$:

$$\begin{cases} A(x) &= 2x^3 - 3x^2 + x - 1, \\ B(x) &= 2x^3 - 3x^2 + x + 1, \\ C(x) &= -2x^3 + 3x^2 + x - 1. \end{cases}$$

et

$$f_{21}(x) = A^2(x) + 4x^2(x-1) = B^2(x) - 4x(x-1)^2 = C^2(x) + 8x^2(x-1)^2.$$

Notons D_0, D_1, D_∞ les diviseurs rationnels sur la courbe E

$$\begin{aligned} D_0 &= (0, A(0)) - (+\infty) = (0,-1) - (+\infty), \\ D_1 &= (1, A(1)) - (+\infty) = (1,-1) - (+\infty), \\ D_\infty &= (-\infty) - (+\infty), \end{aligned}$$

et soient $\varphi_1(x,y) = y - A(x)$, $\varphi_2(x,y) = \frac{y-B(x)}{x(x-1)}$ et $\varphi_3(x,y) = \frac{y-C(x)}{(x-1)^2}$.
Le calcul montre que

$$\begin{pmatrix} (\varphi_1) \\ (\varphi_2) \\ (\varphi_3) \end{pmatrix} = \begin{pmatrix} 2 & 1 & -3 \\ -1 & -2 & 0 \\ 2 & -2 & 1 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix}$$

Donc la classe du diviseur D_0 est d'exposant 21. En effet,

$$\left(\frac{{\varphi_1}^2 {\varphi_3}^6}{{\varphi_2}^5} \right) = 21 D_0.$$

Par conséquent l'ordre de la classe de D_0 est 1, 3, 7 ou 21. Si cet ordre était 1, la courbe serait de genre 0 et le discriminant de f_{21} serait nul. Or ce discriminant est $-2^{17}13^2 \neq 0$, ce qui prouve que l'ordre de la classe de D_0 n'est pas 1.
Supposons que l'ordre de la classe de D_0 soit 3. Le diviseur de la fonction $\varphi_1\varphi_3$ est $4D_0 - D_1 - 2D_\infty$, donc $D_0 - D_1 - 2D_\infty \sim 0$. Or $(\varphi_2) = -D_0 - 2D_1$, donc

$$2D_0 + D_1 - 2D_\infty \sim 0.$$

Posons $P_0 = (0, A(0))$ et $P_1 = (1, A(1))$. On a donc

$$2(P_0) + (P_1) - 2(-\infty) - (+\infty) \sim 0,$$

ce qui nécessite l'existence d'une fonction $\chi \in L(2(-\infty) + (+\infty))$. Une telle fonction est un polynôme de degré 2 en x, qui a donc nécessairement un pôle double en $+\infty$; par conséquent l'ordre de la classe de D_0 n'est pas 3.
Supposons enfin que l'ordre de la classe de D_0 soit 7. En utilisant à nouveau le diviseur de la fonction $\varphi_1\varphi_3$, il vient

$$-3D_0 - D_1 - 2D_\infty \sim 0.$$

Par ailleurs, $D_0 + 2D_1 \sim 0$. Donc

$$-2D_0 + D_1 - 2D_\infty \sim 0,$$

Or

$$(\varphi_3) = 2D_0 - 2D_1 + D_\infty,$$

donc

$$-D_1 - D_\infty \sim 0,$$

i.-e.

$$(P_1) + (-\infty) - 2(+\infty) \sim 0,$$

ce qui est impossible.

Nous avons donc montré que l'ordre de la classe de D_0 est 21.

Notons α, β, γ (resp. $\alpha_{21}, \beta_{21}, \gamma_{21}$) les invariants absolus, déduits des invariants d'Igusa (*cf.* [2], p. 772), de la courbe $X_1(18)$ (resp. C_{21}). Leurs valeurs sont :

$$\begin{aligned} (\alpha, \beta, \gamma) &= (\frac{21}{80}, \frac{17}{1600}, \frac{1}{9375}), \\ (\alpha_{21}, \beta_{21}, \gamma_{21}) &= (\frac{1091}{13872}, \frac{3161}{166464}, \frac{676}{345025251}). \end{aligned}$$

Par conséquent les courbes $X_1(18)$ et C_{21} ne sont pas $\overline{\mathbf{Q}}$-isomorphes.

Notons que nous avons obtenu (*cf.* [2]), par une méthode différente, une infinité de courbes de genre 2, définies sur $\mathbf{Q}$, deux à deux non $\overline{\mathbf{Q}}$-isomorphes, et dont la jacobienne possède un point rationnel d'ordre 21. La courbe que nous avons obtenu ci-dessus n'est pas $\mathbf{Q}$-isomorphe à l'une des courbes décrites dans [2] : ces courbes étaient en effet munies d'un point de Weierstraß rationnel, tandis que C_{21} en est dépourvue.

Dans les deux paragraphes suivants, nous décrivons, de manière plus succinte, l'application de la méthode à l'obtention des courbes du théorème **1.2.1**.

2.2. Les autres valeurs de l. Les courbes C_{22}, C_{26} et $C_{24,1}$.

Avec les notations du début du paragraphe **2**, le choix $(\alpha_1, \beta_1) = (3, 1)$ et $(\alpha_2, \beta_2) = (1, 3)$ mène aux courbes C_{22}, C_{26} et $C_{24,1}$. Ainsi, en cherchant une courbe pour laquelle $(\alpha_3, \beta_3) = (2, 2)$, on obtient la courbe C_{22} dont une équation est

$$y^2 = f_{22}(x) = A^2(x) - 8x^3(x-1) = B^2(x) + 8x(x-1)^3 = C^2(x) + 16x^2(x-1)^2,$$

avec

$$\begin{cases} A(x) &= 2x^3 - 2x^2 + 3x - 2, \\ B(x) &= 2x^3 - 2x^2 - x + 2, \\ C(x) &= -2x^3 + 2x^2 + 3x - 2. \end{cases}$$

Les diviseurs rationnels considérés sont

$$D_0 = (0,-2) - (+\infty), \qquad D_1 = (1,1) - (+\infty), \qquad D_\infty = (-\infty) - (+\infty),$$

et, si $\varphi_1(x,y) = y - A(x)$, $\varphi_2(x,y) = \frac{y-B(x)}{x}$ et $\varphi_3(x,y) = y - C(x)$, le calcul montre que

$$\begin{pmatrix} (\varphi_1) \\ (\varphi_2) \\ (\varphi_3) \end{pmatrix} = \begin{pmatrix} 3 & 1 & -3 \\ -1 & 3 & -2 \\ 2 & 2 & -1 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix}$$

Il est alors facile, comme dans la section **2.1**, de montrer que l'ordre de la classe de D_0 est effectivement 22.
De même, avec $(\alpha_3, \beta_3) = (1,1)$, on obtient la courbe C_{26} dont une équation est

$$y^2 = f_{26}(x) = A^2(x)+24x^3(x-1) = B^2(x)+72x(x-1)^3 = C^2(x)+96x(x-1),$$

avec

$$\begin{cases} A(x) &= \quad 6x^3 - 18x^2 + 11x - 2, \\ B(x) &= \quad 6x^3 - 18x^2 + 7x + 2, \\ C(x) &= \quad -6x^3 + 18x^2 - 13x - 2. \end{cases}$$

Les diviseurs rationnels considérés sont

$$D_0 = (0,-2) - (+\infty), \qquad D_1 = (1,-3) - (+\infty), \qquad D_\infty = (-\infty) - (+\infty),$$

et, si $\varphi_1(x,y) = y - A(x)$, $\varphi_2(x,y) = \frac{y-B(x)}{x}$ et $\varphi_3(x,y) = y - C(x)$, le calcul montre que

$$\begin{pmatrix} (\varphi_1) \\ (\varphi_2) \\ (\varphi_3) \end{pmatrix} = \begin{pmatrix} 3 & 1 & -3 \\ -1 & 3 & -2 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix}$$

et l'on vérifie que l'ordre de la classe de D_0 est 26.
Enfin, avec $(\alpha_3, \beta_3) = (2,0)$, on trouve la courbe $C_{24,1}$, dont une équation est

$$y^2 = f_{24,1}(x) = A^2(x) - 8x^3(x-1) = B^2(x) - 24x(x-1)^3 = C^2(x) - 48x^2,$$

ou encore

$$f_{24,1}(x) = (2x^2 - 2x - 1)(2x^4 - 10x^3 + 7x^2 + 4x - 4),$$

avec

$$\begin{cases} A(x) &= \quad 2x^3 - 6x^2 + x + 2, \\ B(x) &= \quad (x-2)(2x^2 - 2x + 1), \\ C(x) &= \quad -2x^3 + 6x^2 + x + 2. \end{cases}$$

Les diviseurs rationnels considérés sont

$$D_0 = (0,2) - (+\infty), \qquad D_1 = (1,-1) - (+\infty), \qquad D_\infty = (-\infty) - (+\infty),$$

et, si $\varphi_1(x,y) = y - A(x)$, $\varphi_2(x,y) = \frac{y-B(x)}{x}$ et $\varphi_3(x,y) = y - C(x)$, le calcul montre

$$\begin{pmatrix} (\varphi_1) \\ (\varphi_2) \\ (\varphi_3) \end{pmatrix} = \begin{pmatrix} 3 & 1 & -3 \\ -1 & 3 & -2 \\ 2 & 0 & 1 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix}$$

On vérifie alors que la classe de D_0 est d'ordre 24.

La courbe $C_{24,2}$.

Nous avons obtenu une seconde courbe de genre 2 dont la jacobienne possède un point rationnel d'ordre 24, à partir des exposants $(\alpha_1, \beta_1) = (3,2)$, $(\alpha_2, \beta_2) = (2,2)$ et $(\alpha_3, \beta_3) = (1,0)$. Une équation de cette courbe est

$$y^2 = f_{24,2}(x) = A^2(x) + 4x^3(x-1)^2 = B^2(x) + 12x^2(x-1)^2 = C^2(x) - 12x,$$

ou encore

$$f_{24,2}(x) = (x^2 - x + 1)(x^4 - 3x^2 + 8x^2 - 3x + 1),$$

avec

$$\begin{cases} A(x) &= x^3 - 4x^2 + 2x - 1 \\ B(x) &= (x+1)(x^2 - 3x + 1) \\ C(x) &= x^3 - 2x^2 + 4x + 1 \end{cases}$$

Le discriminant de $f_{24,2}(x)$ est $-2^{14}3^3 5^2 \neq 0$, donc cette courbe est de genre 2. Par ailleurs, les diviseurs rationnels considérés sont

$$D_0 = (0,-1) - (+\infty), \qquad D_1 = (1,-2) - (+\infty), \qquad D_\infty = (-\infty) - (+\infty),$$

et, si $\varphi_1(x,y) = y - A(x)$, $\varphi_2(x,y) = \frac{y-B(x)}{x^2}$ et $\varphi_3(x,y) = \frac{y-C(x)}{x}$, le calcul montre que

$$\begin{pmatrix} (\varphi_1) \\ (\varphi_2) \\ (\varphi_3) \end{pmatrix} = \begin{pmatrix} 3 & 2 & -3 \\ -2 & 2 & -1 \\ -1 & 0 & -2 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix}$$

On montre alors que la classe du diviseur rationnel $D = D_0 + D_1$ est d'ordre 24. Les invariants absolus des courbes $C_{24,1}$ et $C_{24,2}$ sont

$$\begin{aligned} (\alpha_{24,1}, \beta_{24,1}, \gamma_{24,1}) &= \left(\frac{7513}{274576}, \frac{199523}{143877824}, -\frac{4968}{38579489651}\right), \\ (\alpha_{24,2}, \beta_{24,2}, \gamma_{24,2}) &= \left(\frac{3529}{132496}, \frac{4321}{529984}, \frac{675}{12480642902}\right), \end{aligned}$$

ce qui montre que les courbes $C_{24,1}$ et $C_{24,2}$ ne sont pas $\overline{\mathbf{Q}}$-isomorphes.
Pour $l = 23, 25, 27$ et 29, nous choisissons les exposants $(\alpha_1, \beta_1) = (3,2)$ et $(\alpha_2, \beta_2) = (2,3)$.

Les courbes C_{25} et C_{27}.

Dans un premier temps, choisissons $(\alpha_3, \beta_3) = (2,0)$. On obtient ainsi, d'une part, la courbe C_{25} dont une équation est

$$y^2 = f_{25}(x) = A^2(x) - 24x^3(x-1)^2 = B^2(x) - 96x^2(x-1)^3 = C^2(x) - 12x^2,$$

avec

$$\begin{array}{rcl} A(x) & = & -6x^3 + 11x^2 - 6x + 3, \\ B(x) & = & -6x^3 + 5x^2 + 6x - 3, \\ C(x) & = & -6x^3 + 13x^2 - 6x + 3. \end{array}$$

Les diviseurs rationnels considérés sur cette courbe sont

$$D_0 = (0,3) - (+\infty), \qquad D_1 = (1,2) - (+\infty), \qquad D_\infty = (-\infty) - (+\infty),$$

et, si $\varphi_1(x,y) = y - A(x)$, $\varphi_2(x,y) = \frac{y-B(x)}{x^2}$ et $\varphi_3(x,y) = y - C(x)$, le calcul montre que

$$\begin{pmatrix} (\varphi_1) \\ (\varphi_2) \\ (\varphi_3) \end{pmatrix} = \begin{pmatrix} 3 & 2 & -2 \\ -2 & 3 & 0 \\ 2 & 0 & 1 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix}$$

On montre alors que l'ordre de la classe de D_0 est 25.
Par ailleurs, on obtient, avec les mêmes exposants, la courbe C_{27} dont une équation est

$$y^2 = f_{27}(x) = A^2(x) - 96x^3(x-1)^2 = B^2(x) - 72x^2(x-1)^3 = C^2(x) - 36x^2,$$

avec

$$\left\{ \begin{array}{rcl} A(x) & = & -2x^3 - 9x^2 + 6x - 3, \\ B(x) & = & -2x^3 - 3x^2 - 6x + 3, \\ C(x) & = & 2x^3 - 15x^2 + 6x - 3. \end{array} \right.$$

Les diviseurs rationnels considérés sur cette courbe sont

$$D_0 = (0,-3) - (+\infty), \qquad D_1 = (1,-8) - (+\infty), \qquad D_\infty = (-\infty) - (+\infty),$$

et, si $\varphi_1(x,y) = y - A(x)$, $\varphi_2(x,y) = \frac{y-B(x)}{x^2}$ et $\varphi_3(x,y) = y - C(x)$, le calcul montre que

$$\begin{pmatrix} (\varphi_1) \\ (\varphi_2) \\ (\varphi_3) \end{pmatrix} = \begin{pmatrix} 3 & 2 & -2 \\ -2 & 3 & 0 \\ 2 & 0 & -3 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix}$$

On vérifie alors que l'ordre de la classe de D_1 est 27.

Les courbes C_{23} et C_{29}.

Choisissons alors $(\alpha_3, \beta_3) = (1,1)$; on obtient ainsi d'une part la courbe C_{23} dont une équation est

$$y^2 = f_{23}(x) = A^2(x) - 16x^3(x-1)^2 = B^2(x) - 8x^2(x-1)^3 = C^2(x) + 32x(x-1),$$

avec

$$\begin{aligned} A(x) &= -x^3 - 3x^2 + 4x - 2, \\ B(x) &= -x^3 + x^2 - 4x + 2, \\ C(x) &= -x^3 + 5x^2 - 4x - 2. \end{aligned}$$

Les diviseurs rationnels considérés sur cette courbe sont

$$D_0 = (0,-2) - (+\infty), \qquad D_1 = (1,-2) - (+\infty), \qquad D_\infty = (-\infty) - (+\infty),$$

et, si $\varphi_1(x,y) = y - A(x)$, $\varphi_2(x,y) = \frac{y - B(x)}{x^2}$ et $\varphi_3(x,y) = y - C(x)$, le calcul montre que

$$\begin{pmatrix} (\varphi_1) \\ (\varphi_2) \\ (\varphi_3) \end{pmatrix} = \begin{pmatrix} 3 & 2 & -2 \\ -2 & 3 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix}$$

Et l'on vérifie que l'ordre de la classe de D_0 est 23.

D'autre part, on obtient, avec les mêmes exposants, la courbe C_{29} dont une équation est

$$y^2 = f_{29}(x) = A^2(x) - 8x^3(x-1)^2 = B^2(x) + 8x^2(x-1)^3 = C^2(x) + 16x(x-1),$$

avec

$$\begin{cases} A(x) = -2x^3 - x^2 + 4x - 2, \\ B(x) = -2x^3 + 3x^2 - 4x + 2, \\ C(x) = 2x^3 - x^2 - 2. \end{cases}$$

Les diviseurs rationnels considérés sur cette courbe sont

$$D_0 = (0,-2) - (+\infty), \qquad D_1 = (1,-1) - (+\infty), \qquad D_\infty = (-\infty) - (+\infty),$$

et, si $\varphi_1(x,y) = y - A(x)$, $\varphi_2(x,y) = \frac{y - B(x)}{x^2}$ et $\varphi_3(x,y) = y - C(x)$, un rapide calcul montre que

$$\begin{pmatrix} (\varphi_1) \\ (\varphi_2) \\ (\varphi_3) \end{pmatrix} = \begin{pmatrix} 3 & 2 & -2 \\ -2 & 3 & 0 \\ 1 & 1 & -3 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix}$$

Et l'on vérifie que l'ordre de la classe de D_0 est 29.

Par ailleurs, comme

$$f_{29}(x) = (2x-1)(2x^5 - x^4 - 4x^2 + 8x - 4),$$

par les transformations habituelles, C_{29} est $\mathbf{Q}$-isomorphe à la courbe d'équation :

$$y^2 = -16x^5 + 33x^4 - 12x^3 + 6x^2 + 4x + 1.$$

2.3. Démonstration du théorème 1.2.2. A partir des exposants $(\alpha_1, \beta_1) = (3,0)$, $(\alpha_2, \beta_2) = (0,3)$ et $(\alpha_3, \beta_3) = (1,1)$, on trouve la courbe C_t dont une équation est

$$y^2 = f(x) = A^2(x) - 4tx^3 = B^2(x) - 4(t-1)(x-1)^3 = C^2(x) + 12t(t-1)x(x-1)$$

soit encore

$$\begin{aligned} y^2 = f(x) \;\; &= \;\; x^6 + 6(t-1)x^5 + 3(t-1)(3t-5)x^4 - (18t^2 - 34t + 18)x^3 \\ &\quad + 3(5t-3)(t-1)x^2 - 6t(t-1)x + t^2, \end{aligned}$$

avec

$$\begin{cases} A(x) &= \quad x^3 + 3(t-1)x^2 + 3(1-t)x + t \\ B(x) &= -x^3 + 3(1-t)x^2 - 3(1-t)x + 2 - t \\ C(x) &= -x^3 + 3(1-t)x^2 - 3(1-t)x + t \end{cases}$$

Les diviseurs rationnels considérés sur cette courbe sont

$$D_0 = (0,t) - (+\infty), \qquad D_1 = (1, 1-t) - (+\infty), \qquad D_\infty = (+\infty) - (-\infty),$$

et, si $\varphi_1(x,y) = y - A(x)$, $\varphi_2(x,y) = y - B(x)$ et $\varphi_3(x,y) = \frac{y - C(x)}{x-1}$, un rapide calcul montre que

$$\begin{pmatrix} (\varphi_1) \\ (\varphi_2) \\ (\varphi_3) \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & -3 \\ 1 & -1 & -2 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix}$$

Le diviseur de la fonction ${\varphi_3}^3$ est

$$3D_0 - 3D_1 - 6D_\infty.$$

Or $3D_0 \sim 0$, donc

$$-3D_1 - 6D_\infty \sim 0.$$

Mais

$$(\varphi_2) = 3D_1 - 3D_\infty,$$

donc

$$9D_\infty \sim 0.$$

Par conséquent la jacobienne de la courbe C_t possède un point rationnel d'exposant 3, la classe de D_0, et un point rationnel d'exposant 9, la classe de D_∞.

L'ordre de la classe de D_0 (resp. D_∞) n'est pas 1 car, dans ce cas, le genre de la courbe et le discriminant de f seraient nuls. Tel n'est pas le cas. En effet le discriminant de f par rapport à x est

$$\Delta(f) = -2985984t^6(t-1)^6(t^2-t+1) \neq 0.$$

Supposons que l'ordre de la classe de D_∞ soit 3. L'étude du diviseur de la fonction φ_3 montre qu'alors

$$D_0 - D_1 + D_\infty \sim 0$$

i.-e.

$$(0,t) + (+\infty) - (1, 1-t) - (-\infty) \sim 0.$$

Ceci, *via* la fonction $x-1$, donne l'impossibilité suivante :

$$(0,t) + (1, t-1) - 2(-\infty) \sim 0.$$

Par suite le diviseur D_0 (resp. D_∞) définit un point rationnel d'ordre 3 (resp. 9) de la jacobienne de la courbe C_t.
Montrons que, $\forall k \in \{1, \dots, 8\}$, la classe de $D = kD_\infty$ n'est pas dans le groupe engendré par la classe de D_0.
Si k est premier à 3, c'est évident. Par conséquent supposons $k = 3$ *i.-e.* $D = 3D_\infty$. En premier lieu la classe de D n'est pas d'ordre 1. En effet ceci contredirait le fait que l'ordre de la classe de D_∞ soit 9. Supposons $D \sim D_0$. L'étude du diviseur de la fonction φ_3 montre que $D_\infty - D_1 \sim 0$, ce qui est absurde (le genre de C_t n'est pas nul).
Supposons enfin que $D \sim -D_0$ *i.-e.* $3D_\infty \sim -D_0 \sim 2D_0$. On a

$$({\varphi_3}^2) = 2D_0 - 2D_1 - 4D_\infty$$

donc

$$-2D_1 - D_\infty \sim 0,$$

et $2(1, 1-t) + (+\infty) - 3(-\infty)$ est le diviseur d'une fonction χ que l'on peut supposer être telle que $\chi(x,y) = y - v(x)$, où $v(x) = x^3 + v_2x^2 + v_1x + v_0$. Le point $P_1 = (1, 1-t)$ est un zéro double de χ se traduit par

$$\begin{cases} v_1 &= t + 3 - 2v_0. \\ v_2 &= -2t + v_0 - 3 \end{cases}$$

On a alors l'équation polynômiale

$$f(x) - v^2(x) = (x-1)^2 T_3(x),$$

où T_3 est un élément de $\mathbf{Q}[t,x]$ de degré 3 en x. Le diviseur de la fonction χ est $2(1, 1-t) + (+\infty) - 3(-\infty)$ si et seulement si $T_3(x) = \epsilon$, où ϵ est un élément non nul de $\mathbf{Q}[t]$.

Or $T_3(x) = t_3x^3 + t_2x^2 + t_1x + t_0$, avec

$$\left\{\begin{array}{lcc} t_3 & = & 2(5t - v_0) \\ t_2 & = & -18t + 5t^2 + 4tv_0 + 6v_0 - v_0^2 \\ t_1 & = & -2tv_0 + 2v_0^2 - 4t^2 + 6t - 6v_0 \\ t_0 & = & (t - v_0)(t + v_0) \end{array}\right.$$

On pose donc $v_0 = 5t$, il vient alors

$$T_3(x) = 12tx^2 + 12t(3t-2)x - 24t^2 = 12t(x^2 + (3t-2)x - 2t)$$

qui n'est pas constant. Donc $3D_\infty$ n'est pas équivalent à $-D_0$, et la jacobienne de la courbe C_t possède bien un sous groupe isomorphe à $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z}$. Enfin les invariants absolus de la courbe C_t sont

$$\begin{array}{rcl} \alpha_{C_t} & = & \dfrac{9t^6 - 27t^5 + 110t^4 - 175t^3 + 110t^2 - 27t + 9}{144(t^2 - t + 1)^3} \\ \beta_{C_t} & = & \dfrac{81t^{12} - 486t^{11} + 2985t^{10} - 10470t^9 + 23974t^8 - 38422t^7}{5184(t^2 - t + 1)^6} \\ & & + \dfrac{44757t^6 - 38422t^5 + 23974t^4 - 10470t^3 + 2985t^2 - 486t + 81}{5184(t^2 - t + 1)^6} \\ \gamma_{C_t} & = & \dfrac{t^6(t-1)^6}{157464(t^2 - t + 1)^9} \end{array}$$

α_{C_t} (par exemple) est une fraction rationnelle en t non constante : l'image de la courbe C_t dans la variété de modules des courbes de genre 2 est non constante.
Le corollaire **1.2.3** se déduit immédiatement, par spécialisation du paramètre, du théorème **1.2.2**.

3. Simplicité des jacobiennes des courbes de genre 2.

3.1. Etude des courbes de genre 2 sur des corps finis. Nous renvoyons à [4] pour ce paragraphe. Soient p un nombre premier, g et r des entiers ≥ 1 et $q = p^r$. Considérons une courbe (C), de genre g et ayant bonne réduction modulo p.
Notons, pour $n \geq 1$, N_n le nombre de points de (C) sur le corps $\mathbf{F}_{q^n}$ et $\zeta_C(t)$ la fonction zéta de la courbe (C). Plus précisément

$$\zeta_C(t) = \exp\left(\sum_{n=1}^{\infty} N_n \frac{t^n}{n}\right).$$

La fonction zéta s'écrit également sous la forme

$$\zeta_C(t) = \frac{\prod_{i=1}^{g}(1-\alpha_i t)(1-\bar{\alpha}_i t)}{(1-t)(1-qt)},$$

où, pour $i = 1, \ldots g$, α_i est un élément de $\mathbf{C}$ tel que

$$|\alpha_i| = \alpha_i \bar{\alpha}_i = q.$$

Notons, pour $i \in \{1, \ldots, g\}$, $a_i = \alpha_i + \bar{\alpha}_i$.
Des deux expressions ci-dessus de la fonction zéta, on déduit l'identité

$$N_n = q^n + 1 - \sum_{i=1}^{g}(\alpha_i^n + \bar{\alpha}_i{}^n).$$

Nombre de points de la jacobienne d'une courbe de genre 2 sur un corps fini.
Supposons désormais $g = 2$. Ce qui précède permet de calculer le nombre de points J_q de la jacobienne de (C) sur $\mathbf{F}_q$.
En effet, la connaissance de N_1 et de N_2 permet de déterminer $U = a_1 + a_2$ et $V = a_1 a_2$ par les formules

$$\begin{cases} U &= q+1-N_1 \\ V &= \frac{1}{2}\left((q+1-N_1)^2 - (q^2+4q+1-N_2)\right). \end{cases}$$

a_1 et a_2 sont alors des nombres quadratiques réels conjugués, solutions de

$$P(X) = X^2 - UX + V = 0.$$

Dès lors, on détermine α_1 et α_2. En effet, pour $i = 1, 2$, α_i et $\bar{\alpha}_i$ sont les racines de

$$X^2 - a_i X + q = 0.$$

Enfin le nombre de points de la jacobienne de (C) sur $\mathbf{F}_q$ est

$$J_q = P(q+1) = (q+1)^2 - (q+1)(a_1 + a_2) + a_1 a_2.$$

Un critère d'absolue simplicité de la jacobienne d'une courbe de genre 2 définie sur Q.
Supposons que (C) soit définie sur $\mathbf{Q}$ et ait pour équation

$$y^2 = f(x).$$

Nous pouvons supposer, sans nuire à la généralité, que $f(x) = a_0 x^6 + \cdots + a_6$, où $(a_0, \ldots, a_6) \in \mathbf{Z}^7$.
Nous déduisons de l'étude précédente un critère suffisant d'absolue simplicité de la jacobienne de (C).

Soit p un nombre premier ne divisant pas le discriminant $\Delta(f)$ de f, et notons $\alpha_p, \alpha'_p, a_p, a'_p$ les quantités $\alpha_1, \alpha_2, a_1, a_2$ calculées comme décrit précédemment sur le corps $\mathbf{F}_p$.

LEMME 3.1.1. *Si la jacobienne de (C) est isogène sur une extension de degré n de $\boldsymbol{Q}$ à un produit de courbes elliptiques, alors $\alpha_p^n + \bar{\alpha}_p^n \in \boldsymbol{Z}$.*

En effet, soit K cette extension, $\mathcal{O}_k$ son anneau des entiers, et E_1, E_2 deux courbes elliptiques définies sur K telles qu'il existe une isogénie φ : $Jac(C) \longrightarrow E_1 \times E_2$ définie sur K. Si $\mathcal{P}$ désigne un idéal premier de K au dessus de p, et $\tilde{E}_1$, $\tilde{E}_2$, $\tilde{C}$ les courbes E_1, E_2 et C réduites modulo $\mathcal{P}$, il est clair que les variétés abéliennes $Jac(\tilde{C})$ et $\tilde{E}_1 \times \tilde{E}_2$ sont isogènes sur le corps fini $\mathcal{O}_K/\mathcal{P}\mathcal{O}_K$. Leurs séries L sont alors égales (*cf.* [7]) ; le lemme en découle immédiatement.

Par ailleurs, nous montrons ci-dessous le

LEMME 3.1.2. *Soit $L = \boldsymbol{Q}(\alpha_p)$ et K la clôture galoisienne de L dans $\overline{\boldsymbol{Q}}$. Supposons que le groupe de Galois de $K/\boldsymbol{Q}$ soit le groupe diédral à 8 éléments D_4. Alors la jacobienne de (C) est simple sur $\overline{\boldsymbol{Q}}$.*

Sous les hypothèses du lemme **3.1.2**, $a_p = \alpha_p + \bar{\alpha}_p$ ne peut être entier. Dans le cas contraire l'extension $K/\mathbf{Q}$ serait de degré 2 et l'ordre du groupe de Galois de l'extension $K/\mathbf{Q}$ serait ≤ 2, contrairement à l'hypothèse que $\mathrm{Gal}(K/\mathbf{Q})$ soit le groupe D_4 à 8 éléments.

Par suite a_p n'est pas entier et l'extension $\mathbf{Q}(a_p)/\mathbf{Q}$ est quadratique et réelle.

Par ailleurs, le groupe de Galois de $K/\mathbf{Q}$ étant D_4, l'unique sous-extension de $L/\mathbf{Q}$ de degré 2 est $\mathbf{Q}(a_p)$ qui est donc réelle.

En effet, D_4 possède 3 sous-groupes d'ordre 4 donc distingués (l'indice de chacun est 2). Il leur correspond, par la théorie de Galois, 3 sous-corps de K, L_1, L_2 et L_3, qui sont des extensions quadratiques de $\mathbf{Q}$.

Posons, pour $i = 1, 2$ $L_i = \mathbf{Q}(\sqrt{d_i})$, où d_i est un élément de $\mathbf{Z}$ sans facteurs carrés. Alors $L_3 = \mathbf{Q}(\sqrt{d_3})$, avec $d_3 = d_1 d_2$.

Si $L_1 \subset L$, alors, si L_2 est un sous-corps de L, il en est de même de L_3. Supposons en effet que L_1 et L_2 soient des sous-corps de L. Alors $\sqrt{d_1}$ et $\sqrt{d_2}$ sont des éléments de L. Par suite $\sqrt{d_3} = \sqrt{d_1}\sqrt{d_2} \in L$ et $L_3 \subset L$.

Par conséquent soit L possède au plus un sous-corps L_i, soit L possède les 3 sous-corps L_1, L_2 et L_3. Cette dernière éventualité est impossible.

Par suite L ne peut avoir comme sous-corps plus d'un des L_i. Cependant $\mathbf{Q}(a_p)$ est une sous-extension de L. Comme $\mathbf{Q}(a_p)/\mathbf{Q}$ est quadratique, c'est la seule.

Soit maintenant n un entier ≥ 2 (il a été montré plus haut que $n = 1$ est impossible) tel que $\alpha_p^n + \bar{\alpha}_p^n = A_p \in \mathbf{Z}$. Alors

$$(\alpha_p^n)^2 - A_p(\alpha_p^n) + p^n = 0$$

et α_p^n est un élément de $L = \mathbf{Q}(\alpha_p)$ de degré 1 ou 2.
Comme $[\mathbf{Q}(\alpha_p^n) : \mathbf{Q}] \leq 2$, $\mathbf{Q}(\alpha_p^n)/\mathbf{Q}$ est une sous-extension de $L/\mathbf{Q}$ de degré au plus 2. $\mathbf{Q}(\alpha_p^n)$ est donc égal à $\mathbf{Q}$ ou à $\mathbf{Q}(a_p)$. Dans l'un et l'autre cas α_p^n est un élément de $\mathbf{R}$.
Or

$$\alpha_p = \zeta\sqrt{p},$$

où ζ est un nombre complexe de module 1. Donc

$$\alpha_p^n = p^{\frac{n}{2}}\zeta^n \in \mathbf{R},$$

donc

$$\zeta^n = \pm 1.$$

Par suite $\alpha_p = \zeta\sqrt{p}$ et ζ est un élément de μ_{2n}, le groupe des racines $2n$-ièmes de l'unité. D'autre part $L = \mathbf{Q}(\alpha_p) \subset M = \mathbf{Q}(\sqrt{p}, \zeta)$. Or l'extension $M/\mathbf{Q}$ est galoisienne abélienne, donc $L/\mathbf{Q}$ est galoisien : en effet tout sous-corps d'une extension abélienne de $\mathbf{Q}$ est une extension galoisienne de $\mathbf{Q}$. Mais K, clôture galoisienne de L dans $\overline{\mathbf{Q}}$, est quadratique sur L, donc $L \neq K$. Ceci établit le lemme **3.1.2**.

3.2. Application. Dans ce paragraphe, nous étudions la simplicité des jacobiennes des courbes de genre 2 données dans les théorèmes **1.2.1** et **1.2.2**. Dans certains cas, la méthode décrite dans le paragraphe précédent (dont nous conservons les notations) permet de répondre.
En pratique, K est le corps de décomposition sur $\mathbf{Q}$ du polynôme

$$Q(x) = x^4 - Ux^3 + (V + 2p)x^2 - pUx + p^2 = 0,$$

résultant par rapport à a_p des deux polynômes

$$a_p^2 - Ua_p + V \text{ et } x^2 - a_p x + p.$$

Les courbes C_{21}, $C_{24,2}$ et C_{27}.
Nous montrons ci-dessous que les jacobiennes de C_{21}, $C_{24,2}$ et C_{27} ne sont pas simples sur $\mathbf{Q}$.
Rappelons qu'une équation de C_{21} est :

$$y^2 = f_{21}(x) = 4x^6 - 12x^5 + 13x^4 - 6x^3 + 3x^2 - 2x + 1.$$

Le changement $x \longrightarrow x + \frac{1}{2}$ donne pour équation de C_{21} :

$$y^2 = 16x^6 - 8x^4 + 9x^2 + 2.$$

Notons E_1 la courbe d'équation

$$Y^2 = 16X^3 - 8X^2 + 9X + 2,$$

et E_2 la courbe d'équation

$$Y^2 = 2X^3 + 9X^2 - 8X + 16.$$

Les discriminants des deux membres de droite des équations de E_1 et E_2 sont égaux à $-2^{13}13$: E_1 et E_2 sont donc des courbes elliptiques. Il est facile de voir que E_1 (resp. E_2) est munie d'un point rationnel d'ordre 3 (resp. 7). La courbe C_{21} est en fait un revêtement de E_1 et E_2. De manière explicite $(X = x^2, Y = y)$ et $(X = \frac{1}{x^2}, Y = \frac{y}{x^3})$ sont des revêtements de C_{21} sur respectivement E_1 et E_2.

Par conséquent la jacobienne de C_{21} est isogène sur $\mathbf{Q}$ au produit de deux courbes elliptiques, E_1 et E_2, possédant respectivement un point d'ordre 3 et un point d'ordre 7.

La jacobienne de la courbe C_{21} n'est donc pas simple sur $\mathbf{Q}$ et, *a fortiori*, sur $\overline{\mathbf{Q}}$.

De même, une équation de $C_{24,2}$ est donnée par :

$$y^2 = f_{24,2}(x) = (x^2 - x + 1)(x^4 - 3x^3 + 8x^2 - 3x + 1)$$

soit

$$y^2 = x^6 - 4x^5 + 12x^4 - 14x^3 + 12x^2 - 4x + 1.$$

L'application $(x, y) \longrightarrow (\frac{1}{x}, \frac{y}{x^3})$ est manifestement une involution de $C_{24,2}$. Le changement de variable $(x, y) = (\frac{u-1}{u+1}, \frac{2v}{(u+1)^3})$ mène à l'équation :

$$v^2 = (u^2 + 3)(u^4 - u^2 + 4).$$

Par conséquent, $C_{24,2}$ est clairement un revêtement des courbes elliptiques, notées encore E_1 et E_2, d'équations respectives :

$$\begin{aligned} Y^2 &= (X+3)(X^2 - X + 4), \\ Y^2 &= (1+3X)(1 - X + 4X^2). \end{aligned}$$

On vérifie facilement que E_1 (resp. E_2) possède un point rationnel d'ordre 8 (resp. 3).

La jacobienne de la courbe $C_{24,2}$ n'est donc pas simple sur $\mathbf{Q}$ et, *a fortiori*, sur $\overline{\mathbf{Q}}$.

Enfin, une équation de la courbe C_{27} est donnée par

$$y^2 = f_{27}(x) = (2x^3 - 15x^2 - 3)(2x^3 - 15x^2 + 12x - 3).$$

Le discriminant du membre de droite de l'équation ci-dessus est égal à $2^{32}3^{15}$.

Nous avons calculé modulo p, pour p premier compris entre 5 et 101, les quantités a_p et a'_p. Leurs valeurs, toujours entières, indiquent que la jacobienne de C_{27} n'est probablement pas simple : elle serait donc isogène

à un produit de courbes elliptiques, E et E', munie respectivement d'un point d'ordre 3 et d'un point d'ordre 9.
Nous avons considéré, pour u et v des entiers tels que $v(u-3v)(u^2+3uv+9v^2) \neq 0$, les courbes $E_{u,v}$ d'équation

$$y^2 = 4v^2x^3 + (ux+v)^2.$$

Les courbes $E_{u,v}$ sont alors des courbes elliptiques, munies d'un point d'ordre 3 comme le montre le calcul du diviseur de la fonction $y-(ux+v)$.
Nous avons cherché, en faisant parcourir à u les entiers compris entre 0 et 100 et à v les entiers, premiers à u et $\neq 0$, compris entre -100 et 100, les courbes $E_{u,v}$ ayant 2 et 3 comme uniques places de mauvaise réduction. Parmi celles obtenues, nous avons cherché s'il y en avait dont les a_p, pour p premier égal à $5, 7, \ldots, 101$, coincide avec le a_p ou le a'_p calculé pour la courbe C_{27}. Nous avons ainsi trouvé la courbe $E_{3,-2}$ d'équation

$$Y^2 = 16X^3 + 9X^2 - 12X + 4,$$

$\mathbf{Q}$-isomorphe à la courbe, notée ici E_1, d'équation

$$Y^2 = 648X^3 + 297X^2 + 18X + 1.$$

Nous avons alors cherché à déterminer un revêtement explicite de C_{27} sur E_1 sous la forme $X = \frac{r(x)}{s(x)}$, où $r(x)$ et $s(x)$ sont des éléments de $\mathbf{Z}[t]$ supposés de degré ≤ 3.
Nécessairement, $s(x)$ doit diviser $f_{27}(x)$. Finalement un revêtement explicite est donné par

$$X = \frac{(x-1)^2}{2x^3-15x^2-3},\ Y = \frac{2(x^3-3x^2+15x+3)}{(2x^3-15x^2-3)^2}y.$$

Ceci montre que la jacobienne de C_{27} n'est pas simple sur $\mathbf{Q}$ et, *a fortiori*, sur $\overline{\mathbf{Q}}$.
Les courbes C_{25} et C_t.
La jacobienne de la courbe C_{25} est simple sur $\mathbf{Q}$. Plus précisément, rappelons qu'une équation de C_{25} est donnée par :

$$y^2 = f_{25}(x) = 36x^6 - 156x^5 + 241x^4 - 192x^3 + 102x^2 - 36x + 9.$$

Le discriminant de f_{25} est $\Delta(f_{25}) = 2^{29}3^{12}7^2$. La courbe C_{25} a donc bonne réduction modulo $p = 5$. On obtient les quantités suivantes, calculées sur $\mathbf{F}_5$:

$$\left\{\begin{array}{rcl} U & = & 0 \\ V & = & -11 \\ a_5 & = & \sqrt{11} \\ a'_5 & = & -\sqrt{11} \end{array}\right.$$

Le corps K est donc le corps de décomposition du polynôme

$$Q(x) = x^4 - x^2 + 25.$$

Le groupe de Galois de l'extension $K/\mathbf{Q}$ est V_4, le groupe de Klein. Comme a_5 et a'_5 ne sont pas entiers, cela assure que la jacobienne de C_{25} est simple sur $\mathbf{Q}$.
Les calculs des a_p et a'_p, pour p assez grand, semblent indiquer que la jacobienne de C_{25}, bien que simple sur $\mathbf{Q}$, est isogène, sur $\mathbf{Q}(\sqrt{3})$, à un produit de courbes elliptiques, mais nous n'avons pas de démonstration de ce fait.
De la même manière, nous montrons que la jacobienne de la courbe C_t est simple sur $\mathbf{Q}$.
Rappelons qu'une équation de C_t est donnée par :

$$y^2 = f_t(x)$$

où

$$\begin{aligned} f_t(x) \quad = \quad & x^6 + 6(t-1)x^5 + 3(t-1)(3t-5)x^4 - (18t^2 - 34t + 18)x^3 \\ & +3(t-1)(5t-3)x^2 - 6t(t-1)x + t^2. \end{aligned}$$

La spécialisation de t en 3 mène à la courbe C_3, d'équation :

$$y^2 = x^6 + 12x^5 + 24x^4 - 78x^3 + 72x^2 - 36x + 9.$$

Le discriminant du membre de droite de l'expression ci-dessus est égal à $-2^{18}3^{12}7$. La courbe C_3 a donc bonne réduction modulo $p = 17$. On obtient les quantités suivantes, calculées sur $\mathbf{F}_{17}$:

$$\left\{\begin{array}{rcl} U & = & 0 \\ V & = & -27 \\ a_{17} & = & 3\sqrt{3} \\ a'_{17} & = & -3\sqrt{3} \end{array}\right.$$

Le corps K est donc le corps de décomposition du polynôme

$$Q(x) = x^4 + 7x^2 + 289.$$

Le groupe de Galois de l'extension $K/\mathbf{Q}$ est V_4, le groupe de Klein. Comme a_{17} et a'_{17} ne sont pas entiers, la jacobienne de C_3 est simple sur $\mathbf{Q}$. Nous ne sommes pas parvenus à déterminer si la jacobienne de C_t est absolument simple ou non. Néanmoins, l'étude de C_3 montre que la jacobienne de C_t est génériquement simple sur $\mathbf{Q}$.

Les courbes C_{22}, C_{23}, $C_{24,1}$, C_{26} et C_{29}.

Les jacobiennes de ces courbes sont absolument simples.

En effet, commençons par étudier la courbe C_{22}. Une équation de cette courbe est :

$$y^2 = f_{22}(x) = (2x^2 - 2x + 1)(2x^4 - 2x^3 + x^2 - 4x + 4).$$

Le discriminant de f_{22} est $\Delta(f_{22}) = -2^{26}41$.

La courbe C_{22} a donc bonne réduction modulo $p = 3$. On obtient les quantités suivantes, calculées sur $\mathbf{F}_3$:

$$\begin{cases} U &= \quad -2 \\ V &= \quad -2 \\ a_3 &= -1 + \sqrt{3} \\ a'_3 &= -1 - \sqrt{3} \end{cases}$$

Le corps K est donc le corps de décomposition du polynôme

$$Q(x) = x^4 + 2x^3 + 4x^2 + 6x + 9.$$

Le groupe de Galois de l'extension $K/\mathbf{Q}$ est D_4. En vertu du lemme **3.1.2**, la jacobienne de C_{22} est absolument simple.

Etudions maintenant la courbe C_{23}. Une équation de cette courbe est :

$$y^2 = f_{23}(x) = x^6 - 10x^5 + 33x^4 - 36x^3 + 28x^2 - 16x + 4.$$

Le discriminant de f_{23} est $\Delta(f_{23}) = -2^{27}53$.

La courbe C_{23} a donc bonne réduction modulo $p = 3$. On obtient les quantités suivantes, calculées sur $\mathbf{F}_3$:

$$\begin{cases} U &= \quad -2 \\ V &= \quad -1 \\ a_3 &= -1 + \sqrt{2} \\ a'_3 &= -1 - \sqrt{2} \end{cases}$$

Le corps K est donc le corps de décomposition du polynôme

$$Q(x) = x^4 + 2x^3 + 5x^2 + 6x + 9.$$

Le groupe de Galois de l'extension $K/\mathbf{Q}$ est D_4. En vertu du lemme **3.1.2**, la jacobienne de C_{23} est absolument simple.

Etudions maintenant la courbe $C_{24,1}$. Une équation de cette courbe est :

$$y^2 = f_{24,1}(x) = (2x^2 - 2x - 1)(2x^4 - 10x^3 + 7x^2 + 4x - 4).$$

Le discriminant de $f_{24,1}$ est $\Delta(f_{24,1}) = -2^{28}3^3 23$.

La courbe $C_{24,1}$ a donc bonne réduction modulo $p = 31$. On obtient les quantités suivantes, calculées sur $\mathbf{F}_{31}$:

$$\begin{cases} U &= -8 \\ V &= -32 \\ a_3 &= 4(-1+\sqrt{3}) \\ a'_3 &= 4(-1-\sqrt{3}) \end{cases}$$

Le corps K est donc le corps de décomposition du polynôme

$$Q(x) = x^4 + 8x^3 + 30x^2 + 248x + 961.$$

Le groupe de Galois de l'extension $K/\mathbf{Q}$ est D_4. En vertu du lemme **3.1.2**, la jacobienne de $C_{24,1}$ est absolument simple.

Etudions à présent la courbe C_{26}. Une équation de cette courbe est :

$$y^2 = f_{26}(x) = (6x^2 - 6x + 1)(6x^4 - 30x^3 + 49x^2 - 20x + 4).$$

Le discriminant de f_{26} est $\Delta(f_{26}) = 2^{30}3^{13}5^2$.

La courbe C_{26} a donc bonne réduction modulo $p = 11$. On obtient les quantités suivantes, calculées sur $\mathbf{F}_{11}$:

$$\begin{cases} U &= -2 \\ V &= -12 \\ a_{11} &= -1+\sqrt{13} \\ a'_{11} &= -1-\sqrt{13} \end{cases}$$

Le corps K est donc le corps de décomposition du polynôme

$$Q(x) = x^4 + 2x^3 + 10x^2 + 22x + 121.$$

Le groupe de Galois de l'extension $K/\mathbf{Q}$ est D_4. En vertu du lemme **3.1.2**, la jacobienne de C_{26} est absolument simple.

Enfin une équation de la courbe C_{29} est donnée par :

$$y^2 = f_{29}(x) = (2x - 1)(2x^5 - x^4 - 4x^2 + 8x - 4).$$

Le discriminant de f_{29} est $\Delta(f_{29}) = 2^{26}61$.

La courbe C_{29} a donc bonne réduction modulo $p = 3$. On obtient les quantités suivantes, calculées sur $\mathbf{F}_3$:

$$\begin{cases} U &= -3 \\ V &= 1 \\ a_3 &= \frac{-1+\sqrt{5}}{2} \\ a'_3 &= \frac{-1-\sqrt{5}}{2} \end{cases}$$

Le corps K est donc le corps de décomposition du polynôme

$$Q(x) = x^4 + 3x^3 + 7x^2 + 9x + 9.$$

Le groupe de Galois de l'extension $K/\mathbf{Q}$ est D_4. En vertu du lemme **3.1.2**, la jacobienne de C_{29} est absolument simple.

Bibliographie :

[1] *J. Igusa*, Arithmetic variety of moduli for genus two, *Ann. of Math.* **72** (1960), 612-649.

[2] *F. Leprévost*, Familles de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 15, 17, 19, 21, *C. R. Acad. Sci. Paris.* t. 313, Série I (1991), 771-774.

[3] *F. Leprévost*, Points rationnels de torsion de jacobiennes de certaines courbes de genre 2, *C. R. Acad. Sci. Paris.* t. 316, Série I (1993), 819-821.

[4] *C. Moreno*, Algebraic curves over finite fields, *Cambridge University Press* Cambridge tracts in mathematics **097** (1991).

[5] *A. P. Ogg*, Rational points on certain elliptic modular curves, Providence, Proceedings of Symposia in Pure Mathematics, **24** (1973) 221-231.

[6] *M. A. Reichert*, Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields, *Math. Comp.* **46** (1986), 637-658.

[7] *J. Tate*, Endomorphisms of Abelian Varieties over Finite Fields, *Inv. Math.* **2** (1966), 134-144.

Franck Leprévost
Université Paris 7, Département de Mathématiques,
Tour 45-55, 5ème étage. 2, place Jussieu,
75252 Paris Cedex 05.
e-mail : leprevot@mathp7.jussieu.fr

Franck LEPRÉVOST
Université Paris 7, Département de Mathématiques,
Tour 45-55, 5ème étage. 2, place Jussieu,
75252 Paris Cedex 05.
e-mail: leprevot@mathp7.jussieu.fr