Loi de groupe sur une intersection de deux quadriques

François Brunault

Nous étudions dans cette note la loi de groupe sur une courbe elliptique particulière, donnée comme intersection de deux quadriques. Nous interprétons géométriquement cette loi et, en explicitant des résultats de Lange-Ruppert et Kohel, nous en déterminons toutes les expressions algébriques possibles en degré 2.

Ce texte doit beaucoup à l'enthousiasme et aux nombreuses questions de L.G. Vidiani. Je le remercie vivement pour l'intérêt constant porté à ce texte ainsi que les nombreuses suggestions d'amélioration. Je remercie aussi D. Kohel, qui a accepté de répondre à mes questions.

1. Une démonstration géométrique

On note $(U : V : W : X)$ les coordonnées homogènes de l'espace projectif complexe $\mathbf{P}^3$. On fixe un paramètre $k \in \mathbf{C}^*$. Soit $C \subset \mathbf{P}^3$ l'intersection des deux quadriques projectives suivantes :

$$C : \begin{cases} U^2 - V^2 + kX^2 = 0 \\ W^2 - V^2 - kX^2 = 0 \end{cases} \tag{1}$$

On pose $O_C = (1 : 1 : 1 : 0) \in C$.

Théorème 1.1. — *La courbe C est munie d'une structure de groupe abélien vérifiant les propriétés suivantes :*

(i) *le point O_C est élément neutre ;*

(ii) *l'opposé d'un point $(U : V : W : X)$ de C est $(U : V : W : -X)$;*

(iii) *la somme de deux points $(U_1 : V_1 : W_1 : X_1)$ et $(U_2 : V_2 : W_2 : X_2)$ de C est donnée génériquement par $(U_3 : V_3 : W_3 : X_3)$ avec*

$$\begin{cases} U_3 = U_2V_1W_1X_2 - U_1V_2W_2X_1 \\ V_3 = U_1V_2W_1X_2 - U_2V_1W_2X_1 \\ W_3 = U_1V_1W_2X_2 - U_2V_2W_1X_1 \\ X_3 = U_1^2X_2^2 - U_2^2X_1^2. \end{cases} \tag{2}$$

Dans le cas particulier $k = 1$, la formule (2) apparaît dans [**1**, §8, Exercise 2].

Remarque 1.2. — Le mot « génériquement » est à prendre au sens suivant. Dans certains cas, la formule (2) donne $U_3 = V_3 = W_3 = X_3 = 0$, et ne permet donc pas de calculer la somme des deux points. Les quatre cas à exclure sont les suivants :

$$\begin{aligned}(U_2 : V_2 : W_2 : X_2) \in \big\{&(U_1 : V_1 : W_1 : X_1), (-U_1 : V_1 : -W_1 : X_1), \\ &(U_1 : -V_1 : -W_1 : X_1), (-U_1 : -V_1 : W_1 : X_1)\big\}.\end{aligned}$$

En particulier, la formule (2) n'autorise pas la duplication d'un point. Nous verrons dans la section 2 d'autres expressions de la loi de groupe qui, elles, permettent la duplication. Nous verrons aussi qu'il est vain de chercher une expression de la loi de groupe qui soit définie partout.

Commençons par mettre en bijection C avec une courbe elliptique. Pour cela, effectuons le changement de variables $U' = U - V$ et $W' = W - V$ dans l'équation (1). Il vient

$$C : \begin{cases} 2U'V + U'^2 + kX^2 = 0 \\ 2W'V + W'^2 - kX^2 = 0 \end{cases} \tag{3}$$

En éliminant V, on en tire

$$k(U' + W')X^2 + U'W'(U' - W') = 0. \tag{4}$$

Notons que l'application $(U : V : W : X) \mapsto (U' : W' : X)$ est définie sur $\mathbf{P}^3 - \{O_C\}$, et que sa restriction à $C - \{O_C\}$ est injective puisque V est déterminé par (3) lorsque U' ou W' est non nul.

Étudions maintenant la cubique de $\mathbf{P}^2$ définie par (4). On constate que la droite projective D d'équation $U' + W' = 0$ coupe la cubique au seul point $(U' : W' : X) = (0 : 0 : 1)$. Ce point est donc un point d'inflexion de la cubique. On peut mettre cette dernière sous forme de Weierstraß en envoyant D à l'infini, c'est-à-dire en posant $z = U' + W'$ (on notera $(x : y : z)$ les coordonnées homogènes de $\mathbf{P}^2$). Après quelques calculs, le changement de variables adéquat s'écrit

$$\begin{cases} x = k(U' - W') = k(U - W) \\ y = 2k^2X \\ z = U' + W' = U + W - 2V \end{cases} \tag{5}$$

Il envoie $C - \{O_C\}$ vers la courbe elliptique E donnée par l'équation

$$E : y^2z = x^3 - k^2xz^2. \tag{6}$$

Notons $\varphi : \mathbf{P}^3 - \{O_C\} \to \mathbf{P}^2$ l'application $(U : V : W : X) \mapsto (x : y : z)$. En notant $O_E = (0 : 1 : 0)$ l'unique point à l'infini de E, on a en fait $\varphi(C - \{O_C\}) \subset E - \{O_E\}$ (l'équation $\varphi(U : V : W : X) = O_E$ entraîne $U = W = V$ d'où $X = 0$ et $(U : V : W : X) = O_C$, une contradiction).

On étend φ en une application de C dans E en posant $\varphi(O_C) = O_E$ [1]. D'après ce qui précède, l'application φ est injective sur C. Il n'est pas difficile non plus de voir, à partir de (3) et (4), que $\varphi : C \to E$ est surjective. C'est donc la bijection voulue.

Par transport de structure, C se trouve donc munie d'une structure de groupe abélien dans lequel O_C est élément neutre. La propriété (ii) du théorème 1.1 résulte immédiatement de (5).

1. On peut voir φ comme une projection de centre O_C ; le point $\varphi(O_C)$ s'obtient alors comme l'intersection de la tangente de C en O_C avec la base de la projection.

Il reste à montrer (iii). Pour cela, utilisons le fait que φ est une application projective. Étant donnés trois point P_1, P_2, P_3 de C, on a

$$\varphi(P_1), \varphi(P_2), \varphi(P_3) \text{ alignés } \Leftrightarrow (O_C, P_1, P_2, P_3) \text{ coplanaires.} \tag{7}$$

D'après la définition géométrique de la loi de groupe sur E, la première condition équivaut à $\varphi(P_1) + \varphi(P_2) + \varphi(P_3) = O_E$. En conservant les notations du théorème 1.1(iii), posons $P_i = (U_i : V_i : W_i : X_i)$ pour $i \in \{1, 2\}$ et $P_3 = (U_3 : V_3 : W_3 : -X_3)$. On vérifie que $P_3 \in C$ (cela peut se faire à la main, ou bien avec la commande `NormalForm` de `Maple`, voir ci-après). Grâce à ce qui précède, il suffit alors de montrer que (O_C, P_1, P_2, P_3) sont coplanaires, c'est-à-dire

$$\begin{vmatrix} 1 & U_1 & U_2 & U_3 \\ 1 & V_1 & V_2 & V_3 \\ 1 & W_1 & W_2 & W_3 \\ 0 & X_1 & X_2 & -X_3 \end{vmatrix} = 0. \tag{8}$$

La nullité de ce déterminant peut se vérifier à l'aide d'un logiciel de calcul formel, par exemple `Maple` et son paquet `Groebner`, qui contient la commande `NormalForm` (pour ma part, j'ai évité `Maple` et j'ai vérifié (8) avec `Pari/GP`). Plus précisément, on écrit explicitement le membre de gauche de (8) comme polynôme en les U_i, V_i, W_i, X_i ($1 \leq i \leq 2$), puis on réduit modulo les polynômes $Q_i = U_i^2 - V_i^2 + kX_i^2$ et $R_i = W_i^2 - V^2 - kX_i^2$ ($1 \leq i \leq 2$) (il s'agit de vraies divisions euclidiennes, car les polyômes Q_i et R_i sont unitaires en U_i et W_i respectivement).

2. Détermination de toutes les formules d'addition

Il se trouve que la loi de groupe sur C peut être décrite par des expressions polynomiales autres que (2). Dans cette section, nous allons déterminer toutes les expressions quadratiques possibles de la loi de groupe, en explicitant des techniques de Kohel [**2**].

Soit $\mathbf{C}[U, V, W, X]$ la $\mathbf{C}$-algèbre graduée des polynômes en U, V, W, X. On a une décomposition en somme directe

$$\mathbf{C}[U, V, W, X] = \bigoplus_{d \geq 0} \mathbf{C}[U, V, W, X]_d$$

où $\mathbf{C}[U, V, W, X]_d$ désigne le sous-espace vectoriel des polynômes homogènes de degré d.

Notons $I(C)$ l'idéal de $\mathbf{C}[U, V, W, X]$ engendré par les polynômes $U^2 - V^2 + kX^2$ et $W^2 - V^2 - kX^2$ (appelé *idéal de* C). Comme $I(C)$ est engendré par des polynômes homogènes, on a une décomposition en somme directe $I(C) = \oplus_{d \geq 0} I(C)_d$, où l'on a posé $I(C)_d = I(C) \cap \mathbf{C}[U, V, W, X]_d$.

Considérons la $\mathbf{C}$-algèbre $A(C) = \mathbf{C}[U, V, W, X]/I(C)$ (appelée *algèbre des coordonnées de* C). Si l'on pose $A(C)_d = \mathbf{C}[U, V, W, X]_d/I(C)_d$, alors $A(C)_d$ s'identifie à un sous-espace vectoriel de $A(C)$ et l'on a encore $A(C) = \oplus_{d \geq 0} A(C)_d$. Cette

décomposition fait de $A(C)$ une $\mathbf{C}$-algèbre graduée. Un élément de $A(C)_d$ est dit *homogène de degré d*. Par exemple $A(C)_1 \cong \mathbf{C}[U,V,W,X]_1$ est de dimension 4, tandis que

$$A(C)_2 = \frac{\mathbf{C}[U,V,W,X]_2}{\langle U^2 - V^2 + kX^2, W^2 - V^2 - kX^2\rangle_{\mathbf{C}}}$$

est de dimension 8.

Une *formule d'addition* pour C de bidegré (d_1,d_2) est un quadruplet de polynômes de $\mathbf{C}[U_1,V_1,W_1,X_1,U_2,V_2,W_2,X_2]$, tous homogènes de degré d_i par rapport au groupe de variables (U_i,V_i,W_i,X_i), et définissant la loi de groupe de C presque partout (plus précisément, sur le complémentaire d'un fermé algébrique strict de $C\times C$). Par exemple (2) est une formule d'addition de bidegré $(2,2)$.

Par passage au quotient, une formule d'addition de bidegré (d_1,d_2) définit un quadruplet de $A(C)_{d_1}\otimes_{\mathbf{C}} A(C)_{d_2}$ appelé *loi d'addition* de bidegré (d_1,d_2). Une conséquence immédiate du principe d'homogénéité est que l'ensemble des lois d'addition de bidegré (d_1,d_2), complété par le vecteur nul, forme un sous-espace vectoriel $\mathcal{A}_{d_1,d_2}$ de $(A(C)_{d_1}\otimes_{\mathbf{C}} A(C)_{d_2})^4$.

Kohel [**2**, Thm 6] a démontré que $\mathcal{A}_{2,2}$ est isomorphe à l'espace de Riemann-Roch associé à un certain diviseur effectif symétrique de degré 4 sur C, d'où l'on peut déduire $\dim_{\mathbf{C}}\mathcal{A}_{2,2}=4$. Plus généralement, Kohel [**2**, Corollary 12] montre que pour $d_1,d_2\geq 2$ avec $(d_1,d_2)\neq(2,2)$, on a $\dim_{\mathbf{C}}\mathcal{A}_{d_1,d_2}=16(d_1d_2-d_1-d_2)$. Dans ce texte, nous allons expliciter la preuve de $\dim_{\mathbf{C}}\mathcal{A}_{2,2}=4$ et obtenir en fait une base de $\mathcal{A}_{2,2}$.

Pour commencer, nous allons faire un changement projectif de coordonnées convenable dans $\mathbf{P}^3$. Fixons un point $P=(x:y:1)\in E$. D'après (5), on a

$$\frac{x}{y} = \frac{1}{2k}\left(\frac{U}{X}-\frac{W}{X}\right)$$
$$\frac{1}{y} = \frac{1}{2k^2}\left(\frac{U}{X}+\frac{W}{X}-2\frac{V}{X}\right)$$

De plus

$$\frac{x^2}{y} = \frac{k^2(U-W)^2}{2k^2X(U+W-2V)}. \tag{9}$$

Comme $U^2+W^2=2V^2$, il vient $(U+W)^2+(U-W)^2=4V^2$ et

$$(U+W+2V)(U+W-2V) = (U+W)^2-4V^2 = (U-W)^2,$$

d'où

$$\frac{x^2}{y} = \frac{1}{2}\left(\frac{U}{X}+\frac{W}{X}+2\frac{V}{X}\right).$$

En posant

$$\psi(P) = (1:x:y:x^2) = \left(\frac{1}{y}:\frac{x}{y}:1:\frac{x^2}{y}\right), \tag{10}$$

et $\psi(O_E) = (0:0:0:1)$, on obtient un plongement $\psi : E \to \mathbf{P}^3$. D'après les formules précédentes, ce plongement est linéairement équivalent à $\varphi^{-1} : E \xrightarrow{\cong} C \subset \mathbf{P}^3$, c'est-à-dire qu'il existe une homographie h de $\mathbf{P}^3$ telle que $\psi = h \circ \varphi^{-1}$. En posant $(S:T:Y:Z) = h(U:V:W:X)$, on a explicitement

$$
\begin{aligned}
S &= \frac{1}{k^2}(U + W - 2V) \\
T &= \frac{1}{k}(U - W) \\
Y &= 2X \\
Z &= U + W + 2V
\end{aligned}
\tag{11}
$$

Par définition de h, on a donc $\psi(P) = (S:T:Y:Z)$, ce qui fournit de nouvelles coordonnées sur E. Par le changement de variables ci-dessus, les lois d'addition sur C de bidegré donné, écrites dans les anciennes coordonnées $(U:V:W:X)$, correspondent bijectivement aux lois d'addition sur E de même bidegré, mais écrites dans les nouvelles coordonnées $(S:T:Y:Z)$. Il suffit donc de déterminer ces dernières.

Soit $\mathbf{C}(E)$ le corps des fonctions méromorphes sur E. Pour tout $n \geq 1$, notons $\mathcal{L}_n$ le sous-espace vectoriel de $\mathbf{C}(E)$ formé des fonctions possédant un pôle d'ordre au plus n en O_E, et holomorphes ailleurs. Le théorème de Riemann-Roch donne $\dim \mathcal{L}_n = n$. Par exemple, pour $n = 4$, une base de $\mathcal{L}_4$ est donnée par $(1, x, y, x^2)$. En effet x (resp. y) possède un pôle double (resp. triple) en O_E, et la considération de l'ordre du pôle en O_E montre que cette famille est libre.

Notons $I(E)$ l'idéal de $\mathbf{C}[S,T,Y,Z]$ obtenu à partir de $I(C)$ au moyen du changement de variables (11). L'algèbre $A(E) = \mathbf{C}[S,T,Y,Z]/I(E)$ est encore graduée par le degré, et le changement de variables (11) fournit un isomorphisme d'algèbres graduées $A(E) \cong A(C)$. On définit comme précédemment l'espace des lois d'addition de bidegré $(2,2)$ sur E, que nous noterons $\mathcal{A}'_{2,2}$. Par définition, c'est un sous-espace de $(A(E)_2 \otimes_{\mathbf{C}} A(E)_2)^4$. Par changement de variables, on a encore un isomorphisme $\mathcal{A}_{2,2} \cong \mathcal{A}'_{2,2}$ (noter qu'il importe ici de changer de variables à la fois à la source et à l'arrivée).

Le morphisme d'algèbre $\mathbf{C}[S,T,Y,Z] \to \mathbf{C}(E)$ défini par $S \mapsto 1$, $T \mapsto x$, $Y \mapsto y$ et $Z \mapsto x^2$ se factorise par $A(E)$ et induit un isomorphisme $A(E)_2 \cong \mathcal{L}_8$. Plus généralement, il induit $A(E)_d \cong \mathcal{L}_{4d}$ pour tout $d \geq 1$.

Pour déterminer les lois d'addition, il nous sera nécessaire de considérer des fonctions de deux variables. Nous noterons $\mathbf{C}(E \times E)$ le corps des fonctions méromorphes sur $E \times E$.

Définition 2.1. — Pour tout $n_1, n_2 \geq 1$, notons $\mathcal{M}_{n_1,n_2}$ le sous-espace vectoriel de $\mathbf{C}(E \times E)$ engendré par les fonctions de la forme $(P_1, P_2) \mapsto f(P_1)g(P_2)$ avec $f \in \mathcal{L}_{n_1}$ et $g \in \mathcal{L}_{n_2}$.

Lemme 2.2. — *L'application naturelle $\mathcal{L}_{n_1} \otimes_{\mathbf{C}} \mathcal{L}_{n_2} \to \mathcal{M}_{n_1,n_2}$ est un isomorphisme. En particulier* $\dim_{\mathbf{C}} \mathcal{M}_{n_1,n_2} = n_1 n_2$.

Pour $i \in \{1,2\}$, notons $x_i \in \mathbf{C}(E \times E)$ la fonction $(P_1, P_2) \mapsto x(P_i)$. On définit de même $y_i \in \mathbf{C}(E \times E)$.

Définition 2.3. — Posons

$$\begin{aligned}\theta : \mathcal{L}_4 \times \mathcal{L}_4 &\to \mathbf{C}(E \times E)\\ (f,g) &\mapsto \big((P_1,P_2) \mapsto (x_2 - x_1)^4 f(P_1 - P_2) g(P_1 + P_2)\big).\end{aligned}$$

Lemme 2.4. — *L'application θ est $\mathbf{C}$-bilinéaire et est à valeurs dans $\mathcal{M}_{8,8}$.*

Démonstration. — La bilinéarité de θ est immédiate. Pour $f, g \in \mathcal{L}_4$, montrons $\theta(f,g) \in \mathcal{M}_{8,8}$. L'idée est de montrer que $\theta(f,g)$ est régulière sur $\{(P_1,P_2) \in E \times E; P_1, P_2 \neq O_E\}$. Plus précisément, il s'agit de montrer que les seuls pôles de $\theta(f,g)$ sont les sous-variétés $E \times \{O_E\}$ et $\{O_E\} \times E$, avec au plus ordre 8. Comme f et g sont holomorphes en dehors de l'origine, le seul pôle de la fonction $f(P_1 - P_2)$ (resp. $g(P_1 + P_2)$) est la diagonale Δ (resp. l'anti-diagonale ∇) de $E \times E$. De plus, la fonction $(x_2 - x_1)^4$ possède un zéro d'ordre 4 le long de Δ ainsi que le long de ∇, puisque sur ces ensembles on a $x_1 = x_2$. Ces zéros compensent les pôles de $f(P_1 - P_2)g(P_1 + P_2)$. De plus, les seuls pôles supplémentaires introduits par le facteur $(x_2 - x_1)^4$ sont les sous-variétés $E \times \{O_E\}$ et $\{O_E\} \times E$, chacune avec multiplicité 8 (puisque x possède un pôle double en O_E), d'où le résultat. □

Définition 2.5. — Pour $f \in \mathcal{L}_4$, on pose

$$\Theta(f) = (\theta(f,1), \theta(f,x), \theta(f,y), \theta(f,x^2)) \in \mathcal{M}_{8,8}^4. \tag{12}$$

En combinant l'isomorphisme $A(E)_2 \cong \mathcal{L}_8$ et le lemme 2.2, on obtient un isomorphisme $\mathcal{M}_{8,8} \cong A(E)_2 \otimes_{\mathbf{C}} A(E)_2$.

Proposition 2.6. — *Pour tout $f \in \mathcal{L}_4 - \{0\}$, le quadruplet $\Theta(f)$ est une loi d'addition de bidegré $(2,2)$ sur E. En particulier Θ induit une application linéaire de $\mathcal{L}_4$ vers $\mathcal{A}'_{2,2}$.*

Démonstration. — Voir le début de [**3**, §2]. □

Théorème 2.7. — *L'application $\Theta : \mathcal{L}_4 \to \mathcal{A}'_{2,2}$ est un isomorphisme.*

Démonstration. — Montrons l'injectivité de Θ. L'application $f \mapsto \theta(f,1)$ est en fait déjà injective : si $\theta(f,1) = 0$ alors $f(P_1 - P_2) = 0$ dans $\mathbf{C}(E \times E)$, et il suffit de spécialiser en $P_2 = O_E$ pour obtenir $f = 0$.

Le point difficile est bien sûr la surjectivité de Θ, pour laquelle nous renvoyons à [**2**, Thm 6]. □

L'isomorphisme Θ fournit une description explicite des formules d'addition de bidegré $(2,2)$ sur E : une base de $\mathcal{A}'_{2,2}$ est donnée par exemple par $(\Theta(1), \Theta(x), \Theta(y), \Theta(x^2))$.

Expliquons maintenant comment calculer Θ. D'après ce qui précède, il suffit, pour tout choix de $f, g \in \{1, x, y, x^2\}$, de savoir calculer un représentant de $\theta(f,g) \in A(E)_2 \otimes_{\mathbf{C}} A(E)_2$ dans

$$\mathbf{C}[S_1,T_1,Y_1,Z_1]_2 \otimes_{\mathbf{C}} \mathbf{C}[S_2,T_2,Y_2,Z_2]_2 \subset \mathbf{C}[S_1,T_1,Y_1,Z_1,S_2,T_2,Y_2,Z_2].$$

On procède ainsi : en utilisant les formules d'addition classiques, on exprime les coordonnées de P_1+P_2 et P_1-P_2 en termes de x_1,y_1,x_2,y_2. On obtient ainsi $\theta(f,g)$ comme fonction rationnelle de x_1,y_1,x_2,y_2. En utilisant l'identité $y_i^2 = x_i^3 - k^2x_i$, on peut mettre $\theta(f,g)$ sous la forme suivante :

$$\theta(f,g) = A_{f,g} + B_{f,g}y_1 + C_{f,g}y_2 + D_{f,g}y_1y_2$$

avec $A_{f,g}, B_{f,g}, C_{f,g}, D_{f,g} \in \mathbf{C}(x_1,x_2)$. Le lemme 2.4 assure que $A_{f,g}$, $B_{f,g}$, $C_{f,g}$ et $D_{f,g}$ sont des polynômes en x_1 et x_2, et leurs degrés sont bien contrôlés (puisque les pôles doivent être d'ordre ≤ 8). Il reste alors à écrire $\theta(f,g)$ comme polynôme bihomogène $\widetilde{\theta}(f,g)$ de bidegré $(2,2)$ en $(1,x_1,y_1,x_1^2)$ et en $(1,x_2,y_2,x_2^2)$. En d'autres termes, on remplace chaque occurence de $1,x_i,y_i,x_i^2$ par S_i,T_i,Y_i,Z_i, et ce de manière à obtenir un polynôme homogène de degré 2 par rapport à chaque groupe de variables (le lemme 2.4 assure que c'est possible). On obtient ainsi un représentant

$$\widetilde{\theta}(f,g) \in \mathbf{C}[S_1,T_1,Y_1,Z_1,S_2,T_2,Y_2,Z_2].$$

Exemple 2.8. — Prenons $f=x$ et $g=y$, et calculons un représentant de $\theta(x,y)$. Pari/GP donne l'expression brute suivante de $\theta(x,y)$:

$$\begin{aligned}(x_2-x_1)\theta(x,y) = {} & y_1^5 - y_2y_1^4 + \big[-2y_2^2 + (x_2-x_1)(2x_1^2+x_2x_1-3x_2^2)\big]y_1^3 \\ & + \big[2y_2^3 + (x_2-x_1)(-3x_1^2+3x_2x_1)y_2\big]y_1^2 \\ & + \big[y_2^4 + (x_2-x_1)(3x_2x_1-3x_2^2)y_2^2 \\ & \qquad + (x_2-x_1)(-x_1^5+4x_2^2x_1^3-2x_2^3x_1^2-3x_2^4x_1+2x_2^5)\big]y_1 \\ & + \big[-y_2^5 + (x_2-x_1)(-3x_1^2+x_2x_1+2x_2^2)y_2^3 \\ & \qquad + (2x_1^5-3x_2x_1^4-2x_2^2x_1^3+4x_2^3x_1^2-x_2^5)y_2\big]\end{aligned}$$

En utilisant $y_i^2 = x_i^3 - k^2x_i$, il vient

$$\begin{aligned}\theta(x,y) = {} & \big[k^4(x_2-x_1) + k^2x_2(x_2^2-x_1^2) + x_1x_2^3(x_2-x_1)\big]y_1 \\ & + \big[k^4(x_1-x_2) + k^2x_1(x_1^2-x_2^2) + x_1^3x_2(x_1-x_2)\big]y_2.\end{aligned}$$

On a donc $A_{x,y} = D_{x,y} = 0$ et

$$B_{x,y} = k^4(x_2-x_1) + k^2x_2(x_2^2-x_1^2) + x_1x_2^3(x_2-x_1) \tag{13}$$

$$C_{x,y}(x_1,x_2) = B_{x,y}(x_2,x_1). \tag{14}$$

Un représentant (au sens ci-dessus) de $B_{x,y}y_1$ est donné par

$$R = (k^4T_2S_2 + k^2T_2Z_2)Y_1S_1 + ((-k^2T_2S_2 - T_2Z_2)Z_1 + (-k^4S_2^2 + Z_2^2)T_1)Y_1$$

C'est bien un polynôme bihomogène de bidegré $(2,2)$. Finalement, un représentant de $\theta(x,y)$ est donné en symétrisant R, d'où

$$\begin{aligned}\widetilde{\theta}(x,y) =&(k^4T_2S_2 + k^2T_2Z_2)Y_1S_1 + ((-k^2T_2S_2 - T_2Z_2)Z_1 + (-k^4S_2^2 + Z_2^2)T_1)Y_1\\ &+ (k^4T_1S_1 + k^2T_1Z_1)Y_2S_2 + ((-k^2T_1S_1 - T_1Z_1)Z_2 + (-k^4S_1^2 + Z_1^2)T_2)Y_2\end{aligned}$$

Remarque 2.9. — Un représentant de $\theta(x,y)$ est défini seulement modulo les équations de E, c'est-à-dire modulo la somme des sous-espaces vectoriels $I(E)_2 \otimes \mathbf{C}[S_2,T_2,Y_2,Z_2]_2$ et $\mathbf{C}[S_1,T_1,Y_1,Z_1]_2 \otimes I(E)_2$.

Avec Pari/GP, il est possible d'implémenter le calcul de $\widetilde{\theta}(f,g)$ pour tout $f,g \in \{1,x,y,x^2\}$. Voici les polynômes obtenus :

$$\widetilde{\theta}(1,1) = Z_2^2S_1^2 + 6Z_2S_2Z_1S_1 - 4T_2Z_2T_1S_1 + S_2^2Z_1^2 - 4T_2S_2T_1Z_1$$

$$\begin{aligned}\widetilde{\theta}(1,x) =& -k^2T_2Z_2S_1^2 - 2Z_2Y_2Y_1S_1 + k^2T_2S_2Z_1S_1 - T_2Z_2Z_1S_1\\ &+ k^2Z_2S_2T_1S_1 + Z_2^2T_1S_1 - 2Y_2S_2Z_1Y_1 + 4T_2Y_2T_1Y_1\\ &+ T_2S_2Z_1^2 - k^2S_2^2T_1Z_1 - Z_2S_2T_1Z_1\end{aligned}$$

$$\begin{aligned}\widetilde{\theta}(1,y) =& k^2Z_2Y_2S_1^2 - 3k^2Z_2S_2Y_1S_1 + Z_2^2Y_1S_1 - 3k^2Y_2S_2Z_1S_1\\ &- 3Z_2Y_2Z_1S_1 + 2k^2T_2Y_2T_1S_1 + k^2S_2^2Y_1^2 - 3Z_2S_2Z_1Y_1\\ &+ 2k^2T_2S_2T_1Y_1 + 2T_2Z_2T_1Y_1 + Y_2S_2Z_1^2 + 2T_2Y_2T_1Z_1\end{aligned}$$

$$\begin{aligned}\widetilde{\theta}(1,x^2) =& k^4Z_2S_2S_1^2 + 4k^2T_2Y_2Y_1S_1 + k^4S_2^2Z_1S_1 - 4k^2Z_2S_2Z_1S_1\\ &+ Z_2^2Z_1S_1 + 6k^4T_2S_2T_1S_1 - 6k^2T_2Z_2T_1S_1 - 4T_2Y_2Z_1Y_1\\ &+ 4k^2Y_2S_2T_1Y_1 - 4Z_2Y_2T_1Y_1 + Z_2S_2Z_1^2\\ &- 6k^2T_2S_2T_1Z_1 + 6T_2Z_2T_1Z_1\end{aligned}$$

$$\begin{aligned}\widetilde{\theta}(x,1) =& -k^2T_2Z_2S_1^2 + 2Z_2Y_2Y_1S_1 + k^2T_2S_2Z_1S_1 - T_2Z_2Z_1S_1\\ &+ k^2Z_2S_2T_1S_1 + Z_2^2T_1S_1 + 2Y_2S_2Z_1Y_1 - 4T_2Y_2T_1Y_1\\ &+ T_2S_2Z_1^2 - k^2S_2^2T_1Z_1 - Z_2S_2T_1Z_1\end{aligned}$$

$$\begin{aligned}\widetilde{\theta}(x,x) =& k^4Z_2S_2S_1^2 + k^4S_2^2Z_1S_1 - 4k^2Z_2S_2Z_1S_1 + Z_2^2Z_1S_1\\ &- 2k^4T_2S_2T_1S_1 + 2k^2T_2Z_2T_1S_1 + Z_2S_2Z_1^2\\ &+ 2k^2T_2S_2T_1Z_1 - 2T_2Z_2T_1Z_1\end{aligned}$$

$$\begin{aligned}\widetilde{\theta}(x,y) = &-k^4T_2Y_2S_1^2 + k^4T_2S_2Y_1S_1 + k^2T_2Z_2Y_1S_1 + k^4Y_2S_2T_1S_1\\ &- k^2Z_2Y_2T_1S_1 - k^2T_2S_2Z_1Y_1 - T_2Z_2Z_1Y_1 - k^4S_2^2T_1Y_1\\ &+ Z_2^2T_1Y_1 + T_2Y_2Z_1^2 + k^2Y_2S_2T_1Z_1 - Z_2Y_2T_1Z_1\end{aligned}$$

$$\begin{aligned}\widetilde{\theta}(x,x^2) = &-k^6T_2S_2S_1^2 - 2k^4Y_2S_2Y_1S_1 - k^4T_2S_2Z_1S_1 + k^2T_2Z_2Z_1S_1\\ &- k^6S_2^2T_1S_1 - k^4Z_2S_2T_1S_1 - 2Z_2Y_2Z_1Y_1 - 4k^2T_2Y_2T_1Y_1\\ &+ T_2Z_2Z_1^2 + k^2Z_2S_2T_1Z_1 + Z_2^2T_1Z_1\end{aligned}$$

$$\begin{aligned}\widetilde{\theta}(y,1) = &-k^2Z_2Y_2S_1^2 - 3k^2Z_2S_2Y_1S_1 + Z_2^2Y_1S_1 + 3k^2Y_2S_2Z_1S_1\\ &+ 3Z_2Y_2Z_1S_1 - 2k^2T_2Y_2T_1S_1 + k^2S_2^2Z_1Y_1 - 3Z_2S_2Z_1Y_1\\ &+ 2k^2T_2S_2T_1Y_1 + 2T_2Z_2T_1Y_1 - Y_2S_2Z_1^2 - 2T_2Y_2T_1Z_1\end{aligned}$$

$$\begin{aligned}\widetilde{\theta}(y,x) = &\ k^4T_2Y_2S_1^2 + k^4T_2S_2Y_1S_1 + k^2T_2Z_2Y_1S_1 - k^4Y_2S_2T_1S_1\\ &+ k^2Z_2Y_2T_1S_1 - k^2T_2S_2Z_1Y_1 - T_2Z_2Z_1Y_1 - k^4S_2^2T_1Y_1\\ &+ Z_2^2T_1Y_1 - T_2Y_2Z_1^2 - k^2Y_2S_2T_1Z_1 + Z_2Y_2T_1Z_1\end{aligned}$$

$$\begin{aligned}\widetilde{\theta}(y,y) = &\ k^6T_2S_2S_1^2 - k^4T_2Z_2S_1^2 + 2k^4T_2S_2Z_1S_1 - 2k^2T_2Z_2Z_1S_1\\ &- k^6S_2^2T_1S_1 - 2k^4Z_2S_2T_1S_1 - k^2Z_2^2T_1S_1 + k^2T_2S_2Z_1^2\\ &- T_2Z_2Z_1^2 + k^4S_2^2T_1Z_1 + 2k^2Z_2S_2T_1Z_1 + Z_2^2T_1Z_1\end{aligned}$$

$$\begin{aligned}\widetilde{\theta}(y,x^2) = &-k^6Y_2S_2S_1^2 + k^6S_2^2Y_1S_1 - 3k^4Z_2S_2Y_1S_1 + 3k^4Y_2S_2Z_1S_1\\ &+ 3k^2Z_2Y_2Z_1S_1 + 2k^4T_2Y_2T_1S_1 - 3k^2Z_2S_2Z_1Y_1 + Z_2^2Z_1Y_1\\ &- 2k^4T_2S_2T_1Y_1 - 2k^2T_2Z_2T_1Y_1 - Z_2Y_2Z_1^2 + 2k^2T_2Y_2T_1Z_1\end{aligned}$$

$$\begin{aligned}\widetilde{\theta}(x^2,1) = &\ k^4Z_2S_2S_1^2 - 4k^2T_2Y_2Y_1S_1 + k^4S_2^2Z_1S_1 - 4k^2Z_2S_2Z_1S_1\\ &+ Z_2^2Z_1S_1 + 6k^4T_2S_2T_1S_1 - 6k^2T_2Z_2T_1S_1 + 4T_2Y_2Z_1Y_1\\ &- 4k^2Y_2S_2T_1Y_1 + 4Z_2Y_2T_1Y_1 + Z_2S_2Z_1^2\\ &- 6k^2T_2S_2T_1Z_1 + 6T_2Z_2T_1Z_1\end{aligned}$$

$$\begin{aligned}\widetilde{\theta}(x^2,x) = &-k^6T_2S_2S_1^2 + 2k^4Y_2S_2Y_1S_1 - k^4T_2S_2Z_1S_1 + k^2T_2Z_2Z_1S_1\\ &- k^6S_2^2T_1S_1 - k^4Z_2S_2T_1S_1 + 2Z_2Y_2Z_1Y_1 + 4k^2T_2Y_2T_1Y_1\\ &+ T_2Z_2Z_1^2 + k^2Z_2S_2T_1Z_1 + Z_2^2T_1Z_1\end{aligned}$$

$$\begin{aligned}\widetilde{\theta}(x^2,y) = {} & k^6Y_2S_2S_1^2 + k^6S_2^2Y_1S_1 - 3k^4Z_2S_2Y_1S_1 - 3k^4Y_2S_2Z_1S_1 \\ & - 3k^2Z_2Y_2Z_1S_1 - 2k^4T_2Y_2T_1S_1 - 3k^2Z_2S_2Z_1Y_1 + Z_2^2Z_1Y_1 \\ & - 2k^4T_2S_2T_1Y_1 - 2k^2T_2Z_2T_1Y_1 + Z_2Y_2Z_1^2 - 2k^2T_2Y_2T_1Z_1\end{aligned}$$

$$\widetilde{\theta}(x^2,x^2) = k^8S_2^2S_1^2 + 6k^4Z_2S_2Z_1S_1 + 4k^6T_2S_2T_1S_1 + Z_2^2Z_1^2 + 4k^2T_2Z_2T_1Z_1$$

Grâce au théorème 2.7, on obtient ainsi toutes les lois d'addition de bidegré (2,2) sur E, pour les coordonnées $(S:T:Y:Z)$. En utilisant le changement de variables (11), on en déduit une base de l'espace $\mathcal{A}_{2,2}$ des lois d'addition de bidegré (2,2) sur C (c'est-à-dire pour les coordonnées $(U:V:W:X)$). De manière explicite, une base $(\ell_1,\ell_2,\ell_3,\ell_4)$ de $\mathcal{A}_{2,2}$ est donnée par

$$\begin{aligned}\ell_1 = {} & (U_2^2V_1^2 - kW_2^2X_1^2, U_1U_2V_1V_2 + kW_1W_2X_1X_2, \\ & U_1U_2W_1W_2 + 2kV_1V_2X_1X_2, U_1V_2W_2X_1 + U_2V_1W_1X_2)\end{aligned}$$

$$\begin{aligned}\ell_2 = {} & (U_1U_2V_1V_2 - kW_1W_2X_1X_2, V_1^2V_2^2 + k^2X_1^2X_2^2, \\ & kU_1U_2X_1X_2 + V_1V_2W_1W_2, U_1V_2W_1X_2 + U_2V_1W_2X_1)\end{aligned}$$

$$\begin{aligned}\ell_3 = {} & (U_1U_2W_1W_2 - 2kV_1V_2X_1X_2, -kU_1U_2X_1X_2 + V_1V_2W_1W_2, \\ & V_1^2W_2^2 + kU_2^2X_1^2, U_1V_1W_2X_2 + U_2V_2W_1X_1)\end{aligned}$$

$$\begin{aligned}\ell_4 = {} & (U_1V_2W_2X_1 - U_2V_1W_1X_2, -U_1V_2W_1X_2 + U_2V_1W_2X_1, \\ & - U_1V_1W_2X_2 + U_2V_2W_1X_1, -V_1^2X_2^2 + V_2^2X_1^2)\end{aligned}$$

Remarque 2.10. — La loi d'addition (2) du théorème 1.1 correspond à $-\ell_4$.

Remarque 2.11. — On notera que les expressions de la loi de groupe sont plus simples lorsque l'on utilise les coordonnées $(U:V:W:X)$. Nous n'avons pas d'explication conceptuelle pour ce phénomène. Dans le même ordre d'idées, Kohel a remarqué (fin du §4 de [**2**]) que les lois d'addition les plus simples correspondent, via l'isomorphisme Θ, à des fonctions possédant une symétrie particulière vis-à-vis des translations par les points de 2-torsion de C.

Remarque 2.12. — Il est possible de généraliser les constructions ci-dessus en remplaçant $\mathcal{L}_4$ par $\mathcal{L}_n$ avec $n \geq 3$ quelconque. On peut toujours trouver une base de $\mathcal{L}_n$ formée de monômes du type x^i ou x^iy. Le plongement ψ est alors remplacé par $\psi_n : E \to \mathbf{P}(\mathcal{L}_n) \cong \mathbf{P}^{n-1}$ (pour $n = 3$ et la base $(1,x,y)$ de $\mathcal{L}_3$, on obtient le plongement de Weierstrass standard de E, qui n'est autre que l'inclusion dans $\mathbf{P}^2$). On définit de manière analogue

$$\theta : \mathcal{L}_n \times \mathcal{L}_n \to \mathcal{M}_{2n,2n}.$$

Le théorème 2.7 reste valable, c'est-à-dire que $\Theta : \mathcal{L}_n \to \mathcal{A}'_{2,2}$ est un isomorphisme, de sorte que $\mathcal{A}'_{2,2}$ est de dimension n dans ce cas. Bien sûr, les lois d'addition deviennent rapidement très pénibles à calculer.

Enfin, expliquons comment déterminer, pour une loi d'addition donnée, son ensemble de définition. Revenons pour cela à la définition 2.3 de l'application θ. Tout revient à trouver, pour $f \in \mathcal{L}_4$ fixée, les zéros communs des fonctions méromorphes $\theta(f, g)$ lorsque g parcourt $\mathcal{L}_4$. Notons

$$\mathrm{div}(f) = \Big(\sum_{i=1}^{4}(Q_i)\Big) - 4(O_E)$$

le diviseur des zéros et des pôles de f. Pour $Q \in E$, notons Δ_Q la partie de $E \times E$ définie par :

$$\begin{aligned}\Delta_Q &= \{(P_1, P_2) \in E \times E; P_1 - P_2 = Q\} \\ &= \{(P + Q, P); P \in E\} \subset E \times E.\end{aligned}$$

On constate que la fonction méromorphe $\theta(f, g)$ s'annule sur les sous-variétés Δ_{Q_i} $(1 \leq i \leq 4)$, et ce pour tout $g \in \mathcal{L}_4$. Par suite, l'ensemble de définition de la loi d'addition $\Theta(f)$ est le complémentaire de la réunion des Δ_{Q_i} pour $1 \leq i \leq 4$.

La loi d'addition $\Theta(f)$ autorise la duplication si et seulement si $O_E \notin \{Q_1, Q_2, Q_3, Q_4\}$, c'est-à-dire si et seulement si f a un pôle d'ordre exactement 4 en O_E. Dans l'espace vectoriel $\mathcal{A}'_{2,2}$ des lois d'addition sur E, l'ensemble de celles qui permettent la duplication est donc le complémentaire de l'hyperplan $\Theta(\mathcal{L}_3)$.

Outre la méthode ci-dessus, il est possible de déterminer l'ensemble de définition des lois d'addition ℓ_j de la manière suivante. Il suffit de trouver, pour chaque $j \in \{1, 2, 3, 4\}$, la partie finie S_j de C telle que l'ensemble de définition de ℓ_j soit l'ensemble des couples (P_1, P_2) tels que $P_1 - P_2 \notin S_j$. Pour ce faire, on remplace $(U_2 : V_2 : W_2 : X_2)$ par $(1 : 1 : 1 : 0)$ dans l'expression de ℓ_j. Par exemple pour $j = 1$, la substitution donne $(U_1^2, U_1V_1, U_1W_1, U_1X_1)$. Ce quadruplet est nul si et seulement si $U_1 = 0$. On en déduit

$$S_1 = C \cap \{U = 0\} = \{(0 : \pm\sqrt{k} : \pm\sqrt{2k} : 1)\}.$$

On obtient de même

$$\begin{aligned}S_2 &= C \cap \{V = 0\} = \{(\pm i\sqrt{k} : 0 : \pm\sqrt{k} : 1)\} \\ S_3 &= C \cap \{W = 0\} = \{\pm i\sqrt{2k} : \pm i\sqrt{k} : 0 : 1\} \\ S_4 &= C \cap \{X = 0\} = \{(\pm 1 : \pm 1 : 1 : 0)\}.\end{aligned}$$

Notons que chaque partie S_j est de cardinal 4, et que S_4 n'est autre que l'ensemble des points de 2-torsion de C.

En utilisant les mêmes méthodes, on vérifie que l'ensemble des lois sur C permettant la duplication est le complémentaire dans $\mathcal{A}_{2,2}$ de l'hyperplan engendré par $\ell_1 - \ell_2$, $\ell_2 - \ell_3$ et ℓ_4.

Références

[1] J. W. S. Cassels – *Lectures on elliptic curves*, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991.

[2] D. Kohel – « Addition law structure of elliptic curves », Preprint, `http://arxiv.org/abs/1005.3623`, May 2010.

[3] H. Lange & W. Ruppert – « Complete systems of addition laws on abelian varieties », *Invent. Math.* **79** (1985), no. 3, p. 603–610.

---

6 septembre 2010

François Brunault • *E-mail :* `brunault@umpa.ens-lyon.fr`, ÉNS Lyon, UMPA, 46 allée d'Italie, 69007 Lyon, France