Investigations sur les courbes elliptiques en classe de 12e

Marie-Pierre Falissard, professeure de mathématiques à Pully-Lausanne (collège Champittet)

Le travail décrit ici a été proposé aux élèves préparant le Baccalauréat International[1] dans le cadre de leur "portfolio" (équivalent du Travail de maturité). L'intérêt, d'un point de vue pédagogique, était de combiner des notions intéressantes d'algèbre et d'analyse, impliquant à la fois du calcul numérique et une investigation s'appuyant sur des outils graphiques (tels que Geogebra). Les notions du programme mises en œuvre étaient les suivantes :

- équation du second degré ; polynômes, propriétés de leurs racines ;

- dérivation ; droite tangente en un point ; droites du plan ; propriétés de courbes ;

- notion de groupe (abordée dans une partie optionnelle du cours, "*Ensembles, relations et groupes*", choisie par les élèves concernés).

Il s'agit d'étudier les propriétés remarquables de certaines courbes à équation cubique, propriétés qui sont par ailleurs utilisées couramment en sécurité informatique. Le terme consacré de *courbe elliptique* peut prêter à confusion, puisque ces courbes n'ont pas de rapport avec l'ellipse.

Une courbe cubique donnée ($y^2 = x^3 - 5x + 4$) est étudiée en deux phases.

Dans une première partie, on étudie quelques propriétés de la courbe et on s'attache à valider une conjecture sur les abscisses x_1, x_2 et x_3 des points d'intersection de la courbe avec une droite quelconque : on se rend compte que l'une des abscisses se déduit aisément des deux autres.

Le but de la seconde partie est d'étudier une relation de groupe définie sur les points de la courbe. Elle exploite les résultats de la première partie, puisque cette relation découle de l'intersection de droites avec la courbe précédemment étudiée.

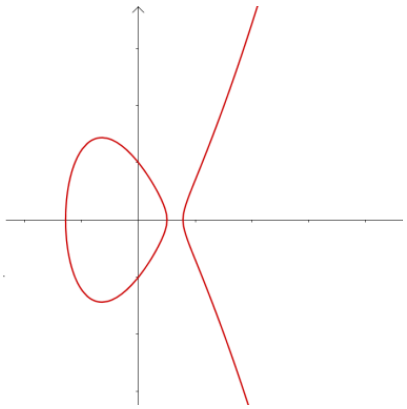
La principale originalité du sujet était cette étude d'une loi de groupe définie sur les points d'une courbe elliptique. Il s'agit là d'un sujet presque "concret", puisque la *cryptographie sur courbe elliptique* (comparable au système RSA mais plus performante) gagne de plus en plus d'importance en sécurité informatique.

On étudie donc la courbe $\mathscr{E}$ formée par les points M (x, y) du plan pour lesquels est vérifiée la relation :

$$y^2 = x^3 - 5x + 4$$

1. Etude de la courbe

Dans une première partie, on s'intéresse à la courbe et à ses intersections avec certaines droites.



L'élève peut tracer la courbe avec Geogebra à partir des fonctions $f(x) = \sqrt{x^3 - 5x + 4}$ et $g(x) = -\sqrt{x^3 - 5x + 4}$.

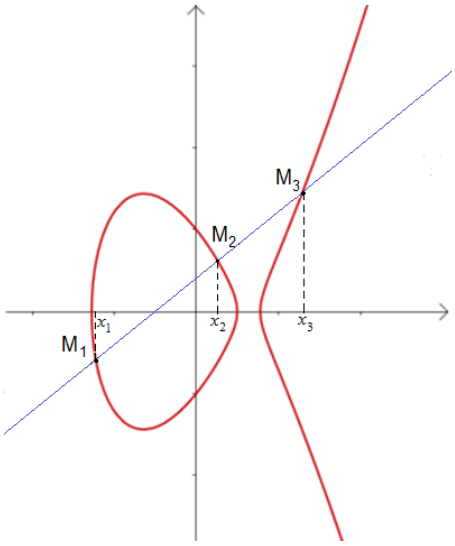
Il remarque que la courbe est en deux parties : une partie fermée, l'autre ouverte. Il en trouve les points remarquables (1, 0), (0, 2), (0, −2).

Il recherche, d'abord graphiquement, puis par le calcul, les abscisses des points d'intersection de $\mathscr{E}$ avec l'axe des abscisses, et trouve aisément les solutions : 1, $\frac{\sqrt{17}-1}{2}$, $\frac{-\sqrt{17}-1}{2}$.

[1] Diplôme de fin d'études secondaires, préparé dans des écoles à vocation internationale, reconnu dans plusieurs pays (principalement anglo-saxons) et ouvrant l'accès à l'université. Actuellement, 35 établissements offrent ce programme en Suisse.

Il s'agit ensuite de s'intéresser graphiquement à l'intersection de $\mathscr{C}$ avec des droites D_a d'équation $y = x + a$. Il y a en général trois points d'intersection, et on cherche à élaborer une conjecture relativement aux abscisses de ces points. Plusieurs essais graphiques (avec différentes valeurs de a) permettent de trouver la relation qui existe entre ces abscisses : leur somme donne toujours 1.

Si maintenant l'on s'intéresse à l'intersection de $\mathscr{C}$ avec d'autres familles de droites, comme les droites D'_a d'équation $y = 2x + a$, on peut de même conjecturer, toujours graphiquement, une relation entre les abscisses des trois points d'intersection : leur somme donne toujours 4.



L'élève peut alors formuler une conjecture plus générale sur les abscisses x_1, x_2 et x_3 des points d'intersection de $\mathscr{C}$ avec une droite d'équation générale $y = px + q$.

La conjecture est que leur somme $x_1 + x_2 + x_3$ donne p^2.

On souhaiterait démontrer cette conjecture dans le cas général. On effectue pour cela un petit détour par la théorie des polynômes, tout en évitant les notions hors programme (telles que les « fonctions symétriques élémentaires des racines du polynôme »). La démonstration ne présente en réalité pas de difficulté pourvu que l'élève soit mis sur la voie.

On étudie d'abord le coefficient a_{n-1} d'un polynôme $P(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ dont on suppose qu'il admet n racines. Une démonstration par récurrence doit fournir la valeur a_{n-1} en fonction des racines de $P(x)$.

La propriété :

« si $P(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ admet n racines, alors a_{n-1} vaut l'opposé de la somme des racines »

est facilement vérifiée pour $n = 1$ et $n = 2$.

On suppose (hypothèse de récurrence) qu'elle est vraie jusqu'à l'ordre $n - 1$.

$P(x)$ ayant n racines peut s'écrire $P(x) = (x - x_n)(x - x_{n-1})... (x - x_1)$,

ce qui peut s'écrire aussi : $(x - x_n)(x^{n-1} - S_{n-1}\,x^{n-2} + ...)$ où S_{n-1} est la somme des racines $x_1 + ... + x_{n-1}$ (d'après l'hypothèse de récurrence).

Le développement du produit donnera $x^n - x_n\,x^{n-1} - S_{n-1}\,x^{n-1} + ...$

Le coefficient du facteur x^{n-1} sera donc $(-x_n - S_{n-1})$, ce qui vérifie l'hypothèse de récurrence à l'ordre n.

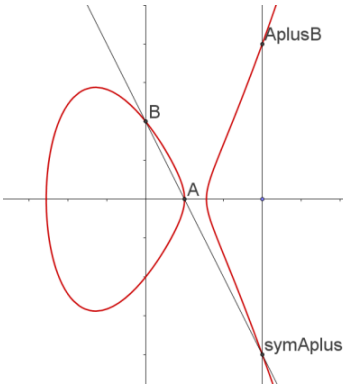
On peut expliquer à l'élève, pour sa culture personnelle, que ces coefficients S_i sont appelés « fonctions symétriques élémentaires des racines du polynôme », et qu'il est établi (mais les démonstrations sont hors programme) que le coefficient a_{n-2} de $P(x)$ vaudra la somme de tous les doubles produits des racines, a_{n-3} l'opposé de la somme de tous les triples produits des racines, etc., jusqu'à a_0 qui vaudra $(-1)^n\,x_1 ... x_{n-1}\,x_n$.

A présent, si l'on remplace y par $px + q$ dans l'équation $y^2 = x^3 - 5x + 4$, et que l'on développe le polynôme du 3e degré résultant, le terme en x^2 aura un coefficient $-p^2$, coefficient qui sera aussi l'opposé de la somme des racines.

La somme des abscisses x_1, x_2 et x_3 des points d'intersection de $\mathscr{C}$ avec une droite d'équation $y = px + q$ est donc bien $\boldsymbol{p^2}$.

L'intérêt de ce résultat est qu'il permet de calculer facilement x_3 quand x_1 et x_2 sont connus (voir seconde partie), ainsi que $y_3 = px_3 + q$. Deux points d'intersection M_1 et M_2 de la courbe et de la droite étant connus, le troisième M_3 s'en déduit facilement. A partir d'une droite (M_1M_2), on peut ainsi construire une correspondance $(M_1,M_2) \rightarrow M_3$.

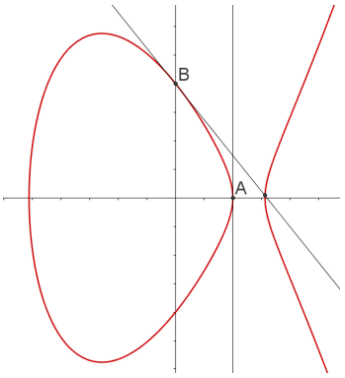
2. Etude d'une loi de groupe définie sur les points de la courbe



Le but de cette partie est d'étudier une relation de groupe, notée par un opérateur $\oplus$, et définie ainsi (loi de groupe sur les points d'une courbe elliptique) :

> Etant donnés deux points quelconques A et B de la courbe $\mathscr{C}$, on note A $\oplus$ B ("AplusB" sur le schéma Geogebra) le point qui est le symétrique par rapport à l'axe des abscisses du point d'intersection de $\mathscr{C}$ avec la droite (AB), quand un tel point existe ("symAplusB" dans Geogebra).

Le cas général A $\oplus$ B est représenté sur la figure ci-contre.



Il faut considérer le cas où les deux points sont confondus. Si A = B, la "droite" (AB) devient la tangente au point A. Cette tangente a généralement une intersection avec $\mathscr{C}$ (exemple du point B sur le schéma ci-contre) sauf si elle est verticale (exemple du point A ci-contre).

L'élève doit enfin repérer les cas où A $\oplus$ B n'est pas défini.

Ces cas se produisent quand les deux points sont sur une même droite verticale, ou quand les deux points sont confondus et ont une ordonnée nulle (tangente verticale).

Quand A $\oplus$ B n'existe pas, on décide de noter A $\oplus$ B = O. Le point O est interprété géométriquement comme « point à l'infini sur l'axe des y ».

L'élève est invité à constater qu'il est alors possible de donner un sens à A $\oplus$ O et O $\oplus$ A. L'intersection de la droite verticale (AO) avec $\mathscr{C}$ sera le symétrique de A par rapport à l'axe des x. Donc A $\oplus$ O redonne A, de même O $\oplus$ A.

Si l'on appelle A' le symétrique de A par rapport à l'axe des x, on a A $\oplus$ A'= A' $\oplus$ A = O. Chaque point de $\mathscr{C}$ a donc un "opposé" dans la loi de groupe, qui est simplement son symétrique par rapport à l'axe des x.

De même, si P est un des trois points d'intersection de $\mathscr{C}$ avec l'axe des abscisses (les trois points vus en première partie), alors P $\oplus$ P a un sens : c'est le point à l'infini O. En ce cas, le point P a pour opposé lui-même.

On a donc bien défini une loi de composition interne sur tous les points de la courbe, en s'aidant d'un « point à l'infini ») fictif qui sert d'élément neutre.

On peut chercher, en utilisant la première partie, à trouver un procédé pour calculer l'abscisse du point $M_1 \oplus M_2$, les deux points M_1 et M_2 étant donnés.

Il faut d'abord calculer l'équation $y = px + q$ de la droite (M_1M_2). Une fois son coefficient directeur p connu, on sait que le point $M_1 \oplus M_2$ aura pour abscisse $x = p^2 - x_1 - x_2$. Son ordonnée sera $-y = -px - q$ puisque c'est le point symétrique de l'intersection de $\mathscr{C}$ avec la droite qui nous intéresse.

On peut utiliser le résultat suivant pour étudier quelques exemples numériques :

> l'équation d'une droite passant par deux points $M_1(x_1 , y_1)$ et $M_2(x_2 , y_2)$ est :
>
> $$y = \frac{y_1 - y_2}{x_1 - x_2} x + \frac{x_1 y_2 - y_1 x_2}{x_1 - x_2} .$$

Si par exemple l'on cherche A ⊕ B, avec A(1, 0) et B(0, 2) :

- la droite (AB) a pour équation $y = -2x + 2$;
- le point A ⊕ B aura pour abscisse $p^2 - x_1 - x_2 = 4 - 1 = 3$, et pour ordonnée $-(-2\times3 + 2) = 4$;
- on a donc A ⊕ B = D (3 ; 4).

Si par exemple l'on cherche le point B ⊕ B avec B(0, 2), il faut s'intéresser à la tangente à la courbe au point B :

- en dérivant $f(x) = \sqrt{x^3 - 5x + 4}$, on trouve que $f'(0) = -\frac{5}{4}$;
- l'équation de la tangente est donc $y = -\frac{5}{4}x + 2$;
- le point B ⊕ B aura pour abscisse $p^2 - x_1 - x_2 = \frac{25}{16} - 0 - 0 = \frac{25}{16}$, et pour ordonnée $-\frac{3}{64}$;
- donc B ⊕ B = (1,5625 ; −0,046875), ce qu'on peut vérifier avec Geogebra (avec la précision adéquate).

Plusieurs propriétés de groupe ayant été établies dans les questions précédentes, on s'intéresse à présent à l'associativité.

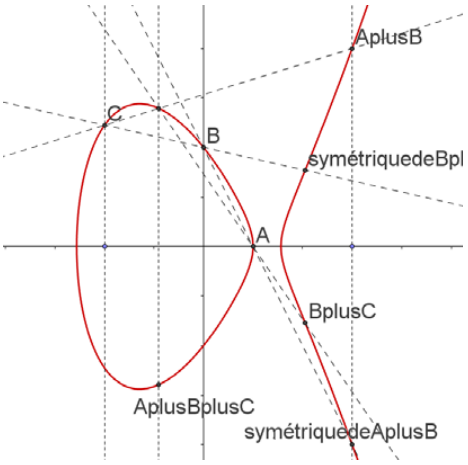
On peut inviter l'élève à la vérifier sur des exemples, en utilisant les points A et B précédents.

Par exemple, pour vérifier que A ⊕ (A ⊕ B) = (A ⊕ A) ⊕ B :

- A ⊕ (A ⊕ B) = A ⊕ D avec A(1, 0) et D (3 ; 4) ; l'équation de la droite (AD) est $y = 2x - 2$; le point A ⊕ D aura donc pour abscisse $p^2 - x_1 - x_2 = 4 - 1 - 3 = 0$ et pour ordonnée 2 : c'est le point B ;

- d'autre part, (A ⊕ A) ⊕ B = O ⊕ B = B.

L'élève est invité alors à vérifier graphiquement, grâce à Geogebra qui permet de déplacer dynamiquement les points sur la courbe, l'associativité de la loi : A ⊕ (B ⊕ C) = (A ⊕ B) ⊕ C, avec A, B et C trois points quelconques de $\mathscr{C}$.



Le schéma correspond ici aux points A(1, 0), B(0, 2) et C(−2,√6)).

Il n'est évidemment pas question de donner une démonstration de cette associativité dans le cas général : cela entraînerait beaucoup trop de calculs, et cela se démontre d'ailleurs autrement.

On propose seulement à l'élève de vérifier analytiquement que les points A ⊕ (B ⊕ C) et (A ⊕ B) ⊕ C sont les mêmes dans le cas suivant : A(1, 0), B(0, 2) et C(−1, −√8).

Le calcul donnera :

- A ⊕ B = (3, 4) et $(A \oplus B) \oplus C = \left(\sqrt{2} - \frac{1}{2}; 3\frac{\sqrt{2}}{4} - \frac{3}{2}\right)$ (soit le point (0.9142137 ; 0.43933911)).
- B ⊕ C = $\left(13 + 8\sqrt{2}; -60 - 42\sqrt{2}\right)$ et $A \oplus (B \oplus C) = \left(\sqrt{2} - \frac{1}{2}; 3\frac{\sqrt{2}}{4} - \frac{3}{2}\right)$.

On a donc pu vérifier sur plusieurs exemples les propriétés de groupe de l'opérateur ⊕ (loi de composition interne, élément neutre, symétriques, associativité), la commutativité étant évidente.

Dans cette étude, on a vu sur un exemple précis les propriétés qui sont au fondement de la *cryptographie sur courbe elliptique*. On peut par la suite expliquer aux élèves que ce procédé cryptographique repose sur la difficulté à retrouver un nombre *n* étant donné un point M de la courbe et le « produit » *n*M lié à la loi de groupe ainsi définie (problème du logarithme discret sur courbe elliptique, les opérations s'effectuant modulo un nombre premier).