Courbes elliptiques

On considère dans tout ce problème, $\mathbb{K}$ est un corps et $\mathbb{K}[X,Y,Z]$ est l'anneau des polynômes à trois indéterminées définie sur $\mathbb{K}$:
$P \in \mathbb{K}[X,Y,Z] \Leftrightarrow$ il existe une famille finie $(a_{i,j,k})$ d'éléments de $\mathbb{K}$ telle que $P(X,Y,Z) = \sum_{i,j,k\in\mathbb{N}} a_{i,j,k}X^iY^jZ^k$.

On appelle degré du monôme $a_{i,j,k}X^iY^jZ^k$ l'entier $i+j+k$
On appelle **degré d'un polynôme** P de $\mathbb{K}[X,Y,Z]$, le plus grand degré de ces monômes.

Définition - Polynôme homogène
On dit que $P \in \mathbb{K}[X,Y,Z]$ est un **polynôme homogène de degré** d, si chacun de ces monômes est de degré d.
Cette définition s'étend sur $\mathbb{K}[X]$ ou $\mathbb{K}[X,Y]$

A. Préliminaires : plan projectif, polynômes homogènes et cubique

On considère $\mathcal{R}$ la relation suivante définie sur $\mathbb{K}^3\backslash\{(0,0,0)\}$:
$(x,y,z)\mathcal{R}(x',y',z')$ si et seulement si $\exists\, t \in \mathbb{K}^*$ tel que $(x,y,z) = t(x',y',z')$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.

On note alors $\mathbb{P}_2(\mathbb{K})$ l'ensemble des classes d'équivalence pour $\mathcal{R}$, appelé plan projectif sur $\mathbb{K}$.

2. Soit $P \in \mathbb{K}[X,Y,Z]$.
Montrer que P homogène de degré d si et seulement si $\forall\ (x,y,z) \in \mathbb{K}^3$, $P(tx,ty,tz) = t^dP(x,y,z)$
3. Considérons maintenant des « points »de la forme $(x,y,0)$ de $\mathbb{P}_2(\mathbb{K})$.
Montrer qu'on peut leur associer simplement (et bijectivement) des directions de droites de $\mathbb{K}^2$.

On appelle alors point à l'infini, le point d'intersection des droites ayant toutes une même direction.

4. Pourquoi, selon vous, appelle-t-on ces points, des points à l'infini ?
Expliquer alors pourquoi on peut écrire : $\mathbb{P}_2(\mathbb{K}) = \mathbb{K}^2 \cup \{\text{directions de droites de } \mathbb{K}^2\}$

Définition - Droite, cubique et courbe elliptique de $\mathbb{P}_2(\mathbb{K})$
Une **droite** $\mathcal{L}$ **de** $\mathbb{P}_2(\mathbb{K})$ est l'ensemble des points $(x,y,z) \in \mathbb{P}_2(\mathbb{K})$ qui satisfait à une relation :
$p(x,y,z) = 0$ où p est un polynôme homogène de degré 1.
Une **cubique** $\mathcal{C}$ **de** $\mathbb{P}_2(\mathbb{K})$ est l'ensemble des points $(x,y,z) \in \mathbb{P}_2(\mathbb{K})$ qui satisfait à une relation :
$p(x,y,z) = 0$ où p est un polynôme homogène de degré 3.
Une **courbe elliptique** $\mathcal{E}$ **de** $\mathbb{P}_2(\mathbb{K})$ est une classe particulière de cubique de $\mathbb{P}_2(\mathbb{K})$.
On montre qu'il s'agit de l'ensemble des points $(x,y,z) \in \mathbb{P}_2(\mathbb{K})$ qui satisfait à une relation :
$p(x,y,z) = 0$ où $p = X^3 - Y^2Z - a_1XYZ + a_2X^2Z - a_3YZ^2 + a_4XZ^2 + a_6Z^3$.
p est un polynôme irréductible sans point singulier.

B. Représentation d'une cubique

L'idée ici est de représenter une courbe elliptique de $\mathbb{P}_2(\mathbb{R})$ sur le plan $\mathbb{R}^2$ auquel on associe un point.
On considère le polynôme $p(X,Y,Z) = X^3 - Y^2Z - 2XZ^2 + 5Z^3$ et l'on note Γ la représentation sur $\mathbb{P}_2(\mathbb{R})$ de la cubique $p(x,y,z) = 0$.

1. Montrer que Γ admet un unique point de la forme $(X,Y,0)$ (i.e. point à l'infini) que l'on précisera.
Nous noterons ce point $\mathcal{O}$. A quelle direction de droite de $\mathbb{R}^2$ ce point est-il rattaché ?
2. Montrer que pour visualiser Γ de $\mathbb{P}_2(\mathbb{R})$ sur $\mathbb{R}^2$,
il suffit d'étudier la courbe γ d'équation $y^2 = x^3 - 2x + 5$, à laquelle on ajoute ce point $\mathcal{O}$.
3. Donner 4 points de γ à coordonnées rationnelles (ou entières).
4. Montrer que le polynôme (à une indéterminée) $\Pi = X^3 - 2X + 5$ n'admet qu'une unique racine sur $\mathbb{R}$.
On représentera schématiquement dans un tableau la courbe d'équation $y = \Pi(x)$.
5. Représenter alors sur $\mathbb{R}^2$ la courbe γ et finalement Γ.
On pourra commencer par montrer qu'elle présente une symétrie d'axe $y = 0$

C. Loi de groupe pour une courbe elliptique

Nous considérons dans cette partie $\mathcal{E}$, un courbe elliptique de $\mathbb{P}_2(\mathbb{K})$ définie par un polynôme $p \in \mathbb{K}[X,Y,Z]$, irréductible et sans point singulier, de la forme $p = X^3 - Y^2Z - a_1XYZ + a_2X^2Z - a_3YZ^2 + a_4XZ^2 + a_6Z^3$.
Notons le résultat suivant (démontré en question 4) :

Proposition -
Soit $\mathcal{L}$, un droite de $\mathbb{P}_2(\mathbb{K})$.
Si $\mathcal{E}$ et $\mathcal{L}$ ont deux points d'intersection (comptés avec leur multiplicité), alors elles ont en réalité trois points d'intersection (comptés avec leur multiplicité).

Définition -Opération $*$ sur $\mathcal{E}$
- Soit P et $Q \in \mathcal{E}$, avec $P \neq Q$. Notons $\mathcal{L}$ la droite (PQ).
  Alors il existe un troisième point de $\mathcal{L}$ appartenant $\mathcal{E}$, nous le notons $P * Q$
- Soit $P \in \mathcal{E}$. Notons $\mathcal{L}$ la droite tangente à $\mathcal{E}$ en P.
  Alors il existe un troisième point de $\mathcal{L}$ appartenant $\mathcal{E}$, nous le notons $P * P$

1. Montrer que la loi $*$ est commutative.
2. Montrons que $\mathcal{O}$ de coordonnées $(0,1,0)$ appartient à $\mathcal{E}$.
   Existe-t-il d'autres points à l'infini dans $\mathcal{E}$?
3. Exprimer, pour tout $P \in \mathcal{E}$, le point $\mathcal{O} * P$ en fonction de P.
4. On démontre ici la proposition 1. Considérons $P_1 = (x_1, y_1, z_1)$ et $P_2 = (x_2, y_2, z_2) \in \mathcal{E}$.
   Notons $\mathcal{L}$, la droite (P_1P_2) de $\mathbb{P}_2(\mathbb{R})$ si $P_1 \neq P_2$ ou bien la droite tangente à $\mathcal{E}$ en P_1 si $P_1 = P_2$.
   $\mathcal{L}$ a pour équation $aX + bY + cZ = 0$
   (a) Montrer que $\mathcal{L} \cap \mathcal{E}$ est un ensemble fini de $\mathbb{P}_2(\mathbb{K})$
   (b) Montrer que l'on peut supposer que : $a = 1$ ou $b = 1$ ou $c = 1$.
   On supposera maintenant que $c = 1$.
   Notons $q = p\big(X, Y, -(aX + bY)\big)$ où p est le polynôme associé à la courbe elliptique $\mathcal{E}$.
   (c) Montrer que q est un polynôme homogène de $\mathbb{K}[X,Y]$. Quel est son degré ?
   On note $\widetilde{q}(X) = q(X,1) \in \mathbb{K}[X]$.
   (d) Montrer que pour tout $(x,y) \in \mathbb{R}^2$, $q(x,y) = y^3\widetilde{q}\left(\dfrac{x}{y}\right)$.
   (e) Cas $P_1 \neq P_2$.
   Calculer $q(x_1, y_1)$ et $q(x_2, y_2)$.
   En déduire que $\widetilde{q} = \left(X - \dfrac{x_1}{y_1}\right)\left(X - \dfrac{x_2}{y_2}\right)(\lambda X + \mu)$.
   En déduire la proposition 1 dans le cas de deux points distincts.
   (f) Expliquer (rapidement) ce qui se passe dans le cas $P_1 = P_2$.
5. Comment visualiser sur la représentation graphique Γ (de la partie B) l'opération $*$ en toute généralité et en particulier $\mathcal{O} * P$?

On admet que $(P_1 * P_2) * (Q_1 * Q_2) = (P_1 * Q_1) * (P_2 * Q_2)$
On pourrait le démontrer par un calcul (géométrie cartésienne ou bien en exploitant des théorèmes de géométrie projective (théorème des neuf points), dans tous les cas, cela demande du temps...

Définition - Opération $+$ sur $\mathcal{E}$
Soit P et $Q \in \mathcal{E}$, alors on note $P + Q = \mathcal{O} * (P * Q)$.

6. Montrer la loi $+$ est commutative.
7. Montrer que $+$ admet un élément neutre.
8. Montrer alors que si $P \in \mathcal{E}$, alors $-P = \mathcal{O} * P$ est le symétrique de P selon la loi $+$
9. Montrer que $P * (Q + R) = (P + Q) * R$ puis que la loi $+$ est associative.
   On pourra utiliser le résultat admis
10. Qu'en déduire quant au couple $(\mathcal{E}, +)$
11. Calculer $(1,-2,1) + (-2,3,-1)$ pour la courbe elliptique définie en B.

Courbes elliptiques - CORRECTION

A. Préliminaires : plan projectif, polynômes homogènes et cubique

1. $\mathcal{R}$ est :
   — réflexive : $(x,y,z) = 1_{\mathbb{K}}(x,y,z)$
   — transitive : $(x,y,z) = t_1(x_1,y_1,z_1)$ et $(x_1,y_1,z_1) = t_2(x_2,y_2,z_2) \Rightarrow (x,y,z) = (t_1 \times t_2)(x_1,y_1,z_1)$
   — symétrique : $(x_1,y_1,z_1) = t(x_2,y_2,z_2) \Rightarrow (x_2,y_2,z_2) = \dfrac{1}{t}(x_1,y_1,z_1)$
   car $\mathbb{K}$ est un corps et tous ses éléments non nuls sont inversibles.

   Ainsi $\mathcal{R}$ est une relation d'équivalence.

On note alors $\mathbb{P}_2(\mathbb{K})$ l'ensemble des classes d'équivalence pour $\mathcal{R}$, il est appelé plan projectif sur $\mathbb{K}$,
cela signifie donc que par exemple $(2,1,3) = (6,3,9)$ dans $\mathbb{P}_2(\mathbb{K})$.

2. On notera que $X - Y$ admet une infinité de racines sans être le polynôme nul (ce sont les (a,a) de $\mathbb{R}^2$).
On n'a donc plus le résultat : P admet une infinité de racines $\Rightarrow P = 0$
et donc : $\big(\forall\, x,y,z \in \mathbb{R},\, P_1(x,y,z) = P_2(x,y,z) \Rightarrow P_1$ et P_2 s'écrivent de la même manière$\big)$ n'est plus évident.

Supposons que P soit homogène de degré d.
Alors chacun des monômes de P est de degré d et donc P est de la forme $\displaystyle\sum_{i+j+k=d} a_{i,j,k}X^iY^jZ^k$.
Et donc $\forall\, x,y,z \in \mathbb{R}$, $\displaystyle P(tx,ty,tz) = \sum_{i+j+k=d} a_{i,j,k}t^{i+j+k}x^iy^jz^k = t^d \sum_{i+j+k=d} a_{i,j,k}x^iy^jz^k = t^dP(x,y,z)$.

Réciproquement, supposons que $\forall\, x,y,z \in \mathbb{R}$, $P(tx,ty,tz) = t^dP(x,y,z)$.
Notons D_1 (resp. D_2, D_3) l'ensemble $\{(i,j,k) \in \mathbb{R}^3 \mid i+j+k = d\}$ (resp. $<,>$).
Alors $P = P_1 + P_2 + P_3$ où $\forall\, i \in \{1,2,3\}$, $\displaystyle P_i = \sum_{(i+j+k)\in D_i} a_{i,j,k}X^iY^jZ^k$.
$\forall\, x,y,z \in \mathbb{R}$, $P_1(tx,ty,tz) + P_2(tx,ty,tz) + P_3(tx,ty,tz) = t^d\big(P_1(x,y,z) + P_2(x,y,z) + P_3(x,y,z)\big)$.
Or comme P_1 est homogène de degré d, on a donc :
$\forall\, x,y,z \in \mathbb{R}$, $\dfrac{1}{t^d}\big(P_2(tx,ty,tz) + P_3(tx,ty,tz)\big) = P_2(x,y,z) + P_3(x,y,z)$.
Ainsi $\dfrac{1}{t^d}\big(P_2(t,t,t) + P_3(t,t,t)\big) = P_2(1,1,1) + P_3(1,1,1)$, constant (en t)
Mais si P_3 n'est pas nul,
$P_2(t,t,t) + P_3(t,t,t)$ est un polynôme en t de degré strictement supérieur à d,
donc $\displaystyle\lim_{t\to+\infty} \frac{1}{t^d}\big(P_2(t,t,t) + P_3(t,t,t)\big) = +\infty$, non constant donc on a une contradiction : $P_3 = 0$.
Puis si P_2 est non nul, on a de même une contradiction pour $t \to 0$, et donc $P_2 = 0$
Par conséquent $P = P_1$ est homogène de degré d.

$\forall\, P \in \mathbb{K}[X,Y,Z]$, P est homogène de degré d ssi $\forall\, (x,y,z) \in \mathbb{K}^3$, $P(tx,ty,tz) = t^dP(x,y,z)$

3. Soit $\varphi : (a,b,0) \to \mathcal{D}$ où $\mathcal{D}$ est la droite d'équation $bx - ay = 0$.
φ est une application bien définie, car si on prend deux représentant de la même classe :
$(a_1,b_1,0)$ et $(a_2,b_2,0)$, alors $\exists\, t \in \mathbb{K}$ tel que $(a_1,b_1,0) = t(a_2,b_2,0)$ et donc comme les équations :
$b_1x - a_1y = 0$ et $tb_1x - ta_1y = 0$, i.e. $b_2x - a_2y = 0$ définissent les mêmes droites,
$\varphi(a_1,b_1,0) = \varphi(a_2,b_2,0)$ et φ ne dépend pas du représentant de la classe d'équivalence.
La bijectivité de φ est obtenue par la définition de l'équation d'une droite de $\mathbb{K}^2$.

Donc on peut associer bijectivement aux "points" de la forme $(x,y,0)$ des directions de droites de $\mathbb{K}^2$.

A noter que cette bijection n'est pas unique...

4. Ces points s'appellent points à l'infini car ils sont définies par une famille de droites parallèles. Le point commun de droites parallèles est obtenu à l'infini (cf. approximation de physique, mais surtout géométrie projective en mathématiques, ou toute sorte de géométrie non euclidienne)
Soient $(x,y,z) \in \mathbb{P}_2(\mathbb{K})$, alors
— ou bien $z = 0$, dans ce cas on associe à $(x,y,0)$ une direction de droites parallèle de $\mathbb{K}^2$

— ou bien $z \neq 0$ dans ce cas un représentant de la même classe que celle de (x, y, z) est $\left(\frac{x}{z}, \frac{y}{z}, 1\right)$.
Et donc on associe (bijectivement) à (x, y, z), le couple $\left(\frac{x}{z}, \frac{y}{z}\right)$ de $\mathbb{K}^2$.

Finalement $\mathbb{P}_2(\mathbb{K}) = \mathbb{K}^2 \cup \{\text{directions de droites de } \mathbb{K}^2\}$

B. Représentation d'une cubique

L'idée ici est de représenter une courbe elliptique de $\mathbb{P}_2(\mathbb{R})$ sur le plan $\mathbb{R}^2$ auquel on associe un point.
On considère le polynôme $p(X, Y, Z) = X^3 - Y^2Z - 2XZ^2 + 5Z^3$ et l'on note Γ la représentation sur $\mathbb{P}_2(\mathbb{R})$ de la cubique $p(x, y, z) = 0$.

1. Soit $(x, y, 0) \in \Gamma$, alors $p(x, y, 0) = 0$ et donc le calcul donne $x^3 = 0$ donc $x = 0$.
Et donc $(x, y, 0)$ est de la forme $(0, y, 0)$. Or dans $\mathbb{P}_2(\mathbb{R})$, il n'y a

qu'un point de cette forme

(ils sont tous dans la même classe d'équivalence), on le notera $\mathcal{O} = (0, 1, 0)$.
$\varphi(0, 1, 0)$ est l'ensemble des droites d'équation $1x - 0y = 0$, donc $x = 0$,

c'est la direction portée par l'axe des ordonnées

2. On suit, pour les points de Γ la décomposition de la fin de première partie :
— le seul point à l'infini est $\mathcal{O}$
— les points de représentant $(x, y, 1)$ vérifient alors $p(x, y, 1) = 0$ c'est à dire $x^3 - y^2 - 2x + 5 = 0$ donc $y^2 = x^3 - 2x + 5$
Donc, en suivant la décomposition de la fin de la première partie,

pour visualiser Γ de $\mathbb{P}_2(\mathbb{R})$ sur $\mathbb{R}^2$, il suffit d'étudier la courbe γ d'équation $y^2 = x^3 - 2x + 5$,
à laquelle on ajoute le point $\mathcal{O}$

3. Les points $(1, 2)$, $(1, -2)$, $(-2, 1)$, $(-2, -1)$, $(2, 3)$ et $(2, -3)$ sont des points de γ.

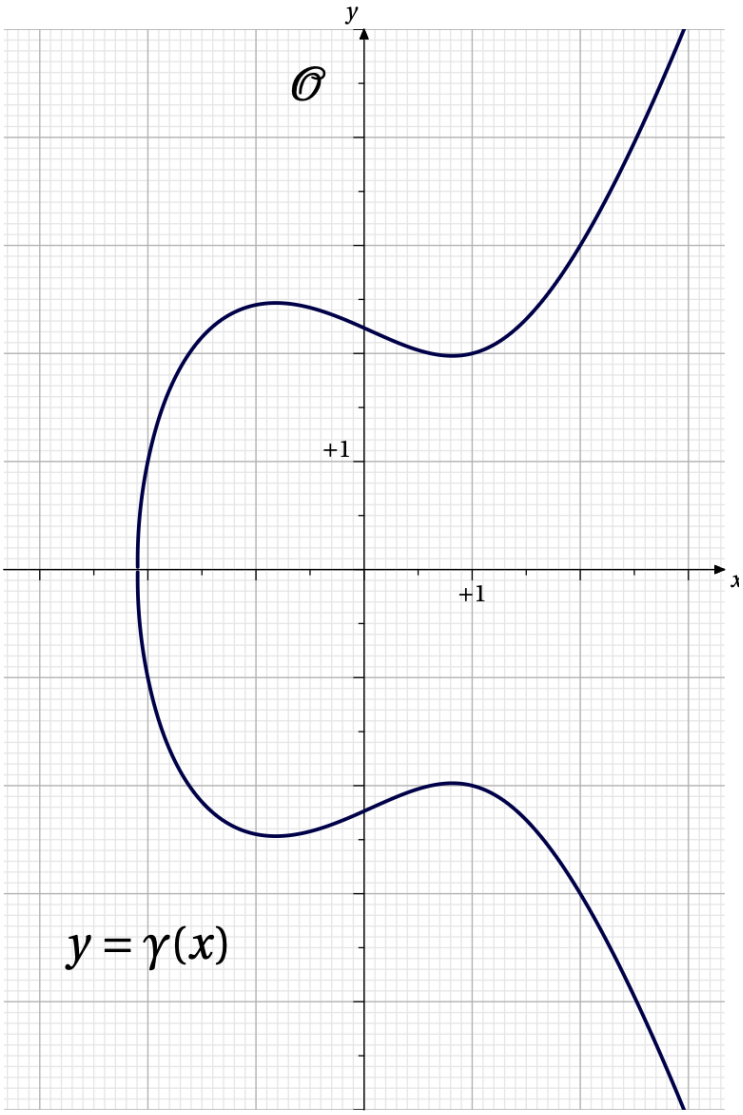
4. $\Pi'(x) = 3x^2 - 2 = 3\left(x - \sqrt{\frac{2}{3}}\right)\left(x + \sqrt{\frac{2}{3}}\right)$. Et $\Pi\left(\sqrt{\frac{2}{3}}\right) = -\frac{1}{3}\sqrt{\frac{2}{3}} + 5 > 0$

x	$-\infty$		$-\sqrt{\frac{2}{3}}$		$\sqrt{\frac{2}{3}}$		$+\infty$
$\Pi'(x)$		$+$	0	$-$	0	$+$	
Π	$-\infty$	$\nearrow$	>0	$\searrow$	>0	$\nearrow$	$+\infty$

D'après le théorème des valeurs intermédiaires,

ce polynôme n'admet qu'une racine sur $\mathbb{R}$ dans $\left]-\infty, -\sqrt{\frac{2}{3}}\right[$.

5. Pour représenter γ, on prend simplement les racines carrées (positive et négative) de $y = \Pi(x)$. Pour obtenir Γ, on ajoute le point à l'infini : point de concours des droites verticales.



C. Loi de groupe pour une courbe elliptique

Nous considérons dans cette partie $\mathcal{E}$, un courbe elliptique de $\mathbb{P}_2(\mathbb{K})$ définie par un polynôme $p \in \mathbb{K}[X, Y, Z]$, irréductible et sans point singulier, de la forme $p = X^3 - Y^2Z - a_1XYZ + a_2X^2Z - a_3YZ^2 + a_4XZ^2 + a_6Z^3$.

1. $P * P = P * P$. Et si $P \neq Q$, alors comme la droite (PQ) est égale à la droite (QP), on a $P * Q = Q * P$.

   Donc la loi $*$ est commutative.

2. Comme pour la partie B, si $\mathcal{E}$ admet un point à l'infini, il est de la forme $(x, y, 0)$, puis le calcul donne $(0, y, 0)$. Tous ces points sont dans la classe de $\mathcal{O}$ de coordonnées $(0, 1, 0)$.
   Réciproquement, ce point est bien un point de $\mathcal{E}$.

   Donc $\mathcal{O}$ de coordonnées $(0, 1, 0)$ est le seul point à l'infini de $\mathcal{E}$.

3. La droite $(\mathcal{O}P)$ est une droite qui passe par $\mathcal{O}$, point de concours des droites verticales. Il s'agit donc d'une droite verticale, celle qui passe par P. Lorsqu'on prolonge cette droite, vu que Γ présente la symétrie $(x, y, 1) \leftrightarrow (x, -y, 1)$, le dernier point de contact est le symétrique de P par rapport à l'axe des abscisses.

   $\mathcal{O} * P$ est le symétrique de P par rapport à l'axe des abscisses.

4. On démontre ici la proposition 1. Considérons $P_1 = (x_1, y_1, z_1)$ et $P_2 = (x_2, y_2, z_2) \in \mathcal{E}$.
Notons $\mathcal{L}$, la droite (P_1P_2) de $\mathbb{P}_2(\mathbb{R})$ si $P_1 \neq P_2$ ou bien la droite tangente à $\mathcal{E}$ en P_1 si $P_1 = P_2$.
$\mathcal{L}$ a pour équation $aX + bY + cZ = 0$

(a) Si $\mathcal{L} \cap \mathcal{E}$ était infini, alors cela signifierait que $aX + bY + cZ$, l'équation de $\mathcal{L}$ diviserait l'équation de $\mathcal{E}$. Or p est irréductible, ceci est donc impossible.

Bilan : $\mathcal{L} \cap \mathcal{E}$ est un ensemble fini de $\mathbb{P}_2(\mathbb{K})$.

(b) $(a, b, c) \neq (0, 0, 0)$, sinon, $\mathcal{L}$ n'est pas bien définie.
A partir de là, l'un des trois coefficients est non nuls, puisque $\mathcal{L}$ est exactement définie par une classe d'équivalence de $\mathbf{P}_2(\mathbb{K})$, on peut choisir celle où ce coefficient non nul vaut exactement 1.

On peut donc supposer que : $a = 1$ ou $b = 1$ ou $c = 1$.

On supposera maintenant que $c = 1$.
Notons $q = p\big(X, Y, -(aX + bY)\big)$ où p est le polynôme associé à la courbe elliptique $\mathcal{E}$.

(c) Pour tout $k \in \mathbb{N}$, $\big(-(aX + bY)\big)^k$ se développe (avec la formule du binôme de Newton) en polynôme homogène de $\mathbb{K}[X, Y]$ de degré k.
Donc $X^iY^j\big(-(aX + bY)\big)^k$ est un polynôme homogène de $\mathbb{K}[X, Y]$ de degré $i + j + k$.
Par conséquent, vue la nature de p :

q est un polynôme homogène de $\mathbb{K}[X, Y]$ de degré 3.

On note $\widetilde{q}(X) = q(X, 1) \in \mathbb{K}[X]$.

(d) q est homogène de degré 3, donc d'après $A.2.$: $\widetilde{q}\left(\dfrac{x}{y}\right) = q\left(\dfrac{x}{y}, 1\right) = q\left(\dfrac{x}{y}, \dfrac{y}{y}\right) = \left(\dfrac{1}{y}\right)^3 q(x, y)$.

Donc pour tout $(x, y) \in \mathbb{R}^2$, $q(x, y) = y^3\widetilde{q}\left(\dfrac{x}{y}\right)$.

(e) Cas $P_1 \neq P_2$. $P_1(x_1, y_1, z_1)$ est un point de $\mathcal{L} \cap \mathcal{E}$, donc on a :
$$\begin{cases} ax_1 + by_1 + z_1 = 0 \\ x_1^3 - y_1^2z_1 - a_1x_1y_1z_1 + a_2x_1^2z_1 - a_3y_1z_1^2 + a_4x_1z_1^2 + a_6z_1^3 = 0 \end{cases}$$
Donc $z_1 = -(ax_1 + by_1)$ et $q(x_1, y_1) = p(x_1, y_1, -(ax_1 + by_1)) = p(x_1, y_1, z_1) = 0$

Ainsi $q(x_1, y_1) = 0$ et de même $q(x_2, y_2) = 0$.

Puisque $\widetilde{q}\left(\dfrac{x_1}{y_1}\right) = \dfrac{1}{y_1^3} \times 0 = 0$, $\widetilde{q}\left(\dfrac{x_2}{y_2}\right) = 0$ et $\widetilde{q}$ est de degré 3, on peut le factoriser :

$\widetilde{q} = \left(X - \dfrac{x_1}{y_1}\right)\left(X - \dfrac{x_2}{y_2}\right)(\lambda X + \mu)$.

$\widetilde{q}$ s'annule en $x_3 = \dfrac{-\mu}{\lambda}$ et donc il existe t tel que p s'annule en $(-t\mu, t\lambda, 1)$,
ce t est unique car il vérifie $-at\mu + bt\lambda + 1 = 0$, donc $t = \dfrac{1}{a\mu - b\lambda}$.
Il existe au moins un troisième point d'intersection de $\mathcal{L}$ et $\mathcal{E}$, le point $P_3(\dfrac{\mu}{a\mu - b\lambda}, \dfrac{\lambda}{-a\mu + b\lambda}, 1)$;
et ce point est unique, sinon on obtiendrait une quatrième racine pour $\widetilde{q}$.

Si il existe deux points distincts sur $\mathcal{L} \cap \mathcal{E}$, alors il en existe nécessairement un et un seul autre,

celui-ci pouvant être un des deux premiers points (P_3 peut-être égale à P_1), mais cela n'est pas génant d'après la règle fixé qui tient compte de la multiplicité éventuelle.
Il a été supposé ici que $y_i \neq 0$, or il peut exister des point de cette forme (les $(x_1, 0, 1)$ où x_1 est solution de $x^3 + a_2x^2 + a_4x + a_6 = 0$), dans ce cas il faudrait mener le même raisonnement mais avec $\widetilde{\widetilde{q}}(Y) = q(1, Y) \in \mathbb{K}[Y]$

(f) Dans ce cas, avec les mêmes notations, on trouve que le polynôme $\widetilde{q}$ est toujours de degré 3 mais de la forme $\left(X - \frac{x_1}{y_1}\right)^2 (\lambda X + \mu)$: il admet une racine double (due à P_1 et P_2) et toujours une troisième racine, ce qui justifie la proposition 1 (dans le cas racine double).

5. Considérons P_1 et P_2 de $\mathcal{E}$.
La droite $\mathcal{L}$ est en fait la droite (P_1P_2), et donc le point $P_3 = P_1 * P2$ est obtenu en traçant le droite (P_1P_2) et en notant le point d'intersection de cette droite avec $\mathcal{E}$.
Si cette droite est tangente en l'un de ces points, celui-ci doit être compté deux fois.
On a déjà vu que $\mathcal{O} * P$ est le symétrique de P par rapport à l'axe des abscisses (la droite $\mathcal{L}$ est ici une droite verticale).

On admet que $(P_1 * P_2) * (Q_1 * Q_2) = (P_1 * Q_1) * (P_2 * Q_2)$
On pourrait le démontrer par un calcul (géométrie cartésienne ou bien en exploitant des théorèmes de géométrie projective (théorème des neuf points), dans tous les cas, cela demande du temps...

Définition - Opération + sur $\mathcal{E}$
Soit P et $Q \in \mathcal{E}$, alors on note $P + Q = \mathcal{O} * (P * Q)$.

6. $P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * (Q * P) = Q + P$, car $*$ est commutatif.

Donc La loi + est commutative.

7. Soit $P \in \mathcal{E}$.
On note $-P$, le symétrique de P par rapport à l'axe des abscisses.
$\mathcal{O} + P = \mathcal{O} * (\mathcal{O} * P) = \mathcal{O} * (-P) = P$ et par commutativité ceci vaut aussi $P + \mathcal{O}$.
Ainsi + admet un élément neutre : $\mathcal{O}$.
8. Soit $P \in \mathcal{E}$.
$P + (-P) = \mathcal{O} * (P * (-P)) = \mathcal{O} * \mathcal{O} = \mathcal{O}$.

Donc $\forall\ P \in \mathcal{E}$, $-P = \mathcal{O} * P$ est le symétrique de P selon la loi +.

9. $P * (Q + R) = P * (\mathcal{O} * (Q * R)) = ((P * Q) * Q) * (\mathcal{O} * (Q * R))$ car $P = (P * Q) * Q$ puisque P, Q et $P * Q$ sont trois points alignés de la courbe elliptique
Et d'après la relation donnée dans l'énoncé :
$P * (Q + R) = ((P * Q) * \mathcal{O}) * (Q * (Q * R)) = (\mathcal{O} * (P * Q)) * R$ car $R = Q * (Q * R)$ (idem)

Ainsi $P * (Q + R) = (P + Q) * R$.

Et en appliquant $\mathcal{O}*$ à chacun des deux membres, on obtient :

$P + (Q + R) = (P + Q) + R$: la loi + est associative.

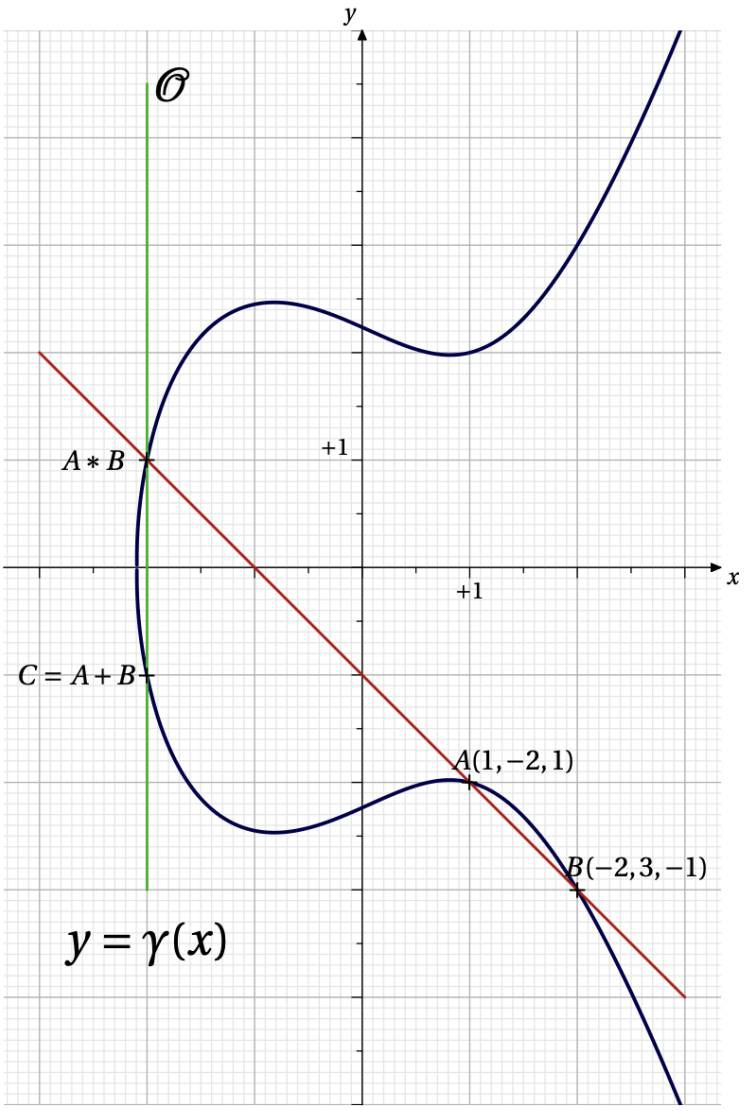
10.

$(\mathcal{E}, +)$ est donc un groupe commutatif (ou abélien).

11. D'abord on transforme l'addition par classe d'équivalence, pour obtenir des points de γ (avec $z = 1$) :
$(1, -2, 1) + (-2, 3, -1) = (1, -2, 1) + (2, -3, 1)$.
Puis on trace la droite qui passe par $A(1, -2)$ et $B(2, -3)$, elle a pour équation $x + y + 1 = 0$.
Elle recoupe la courbe elliptique en $C'(x_3, y_3) = A * B$ vérifiant : $q(x_3, y_3) = 0$.
Ici $q(x, y) = p(x, y, -x - y) = x^3 - y^2(-x - y) - 2x(-x - y)^2 + 5(-x - y)^3$, (avec $\frac{x}{y} = X$ et $\frac{y}{y} = 1$)
$\widetilde{q}(X) = X^3 - (-X - 1) - 2X(-X - 1)^2 + 5(-X - 1)^3 = X^3 + X + 1 - 2X^3 - 4X^2 - 2X - 5X^3 - 15X^2 - 15X - 5$
$\widetilde{q}(X) = -6X^3 - 19X^2 - 16X - 4$ dont on connaÓt deux racines : $\frac{1}{-2}$ et $\frac{2}{-3}$
D'où la factorisation : $\widetilde{q}(X) = -6\left(X + \frac{1}{2}\right)\left(X + \frac{2}{3}\right)(X + 2)$.
On a donc $\frac{x_3}{y_3} = -2$, d'où $C'(-2y_3, y_3)$ avec $x_3 + y_3 + 1 = -y_3 + 1 = 0$.

Ainsi, C' a pour coordonnée $(-2, 1)$.
Puis $C = A + B$ est le symétrique de C', donc $C(-2, -1)$.
Finalement

$(1, -2, 1) + (-2, 3, -1) = (-2, -1, 1)$ pour la courbe elliptique définie en B.



Les courbes elliptiques se retrouvent partout en mathématiques modernes : en arithmétique (cryptologie), en géométrie (grand théorème de Poncelet en géométrie projective), en analyse (complexe, forme modulaire, mais là on retrouve à nouveau la théorie des nombres) . . . Ce problème n'est qu'un avant-goût de ce jardin des délices.