

Épreuve de mathématiques

18 juin 2008 — 2 h 00

Consignes générales aux candidats

- Dès réception du sujet, veuillez vérifier que celui-ci comporte bien le nombre de pages indiqué par l'en-tête. Si vous croyez avoir décelé une erreur :
 1. adressez-vous au jury présent dans la salle ;
 2. signalez soigneusement sur votre copie l'erreur que vous pensez avoir décelé en précisant les raisons de votre appréciation ;
 3. sautez la question, de toute manière vous n'aurez pas le temps de traiter le reste. . .
- Il vous est interdit de signer ou d'apposer un signe distinctif sur votre composition.
- La qualité de la *rédaction* sera prise en compte dans la notation. De plus, on veillera à bien respecter la numérotation des questions et à *encadrer les résultats*.
- Éventuellement, vous pouvez admettre le résultat d'une question précédente pour continuer l'exercice.
- Vous pouvez (et devez), sur l'ensemble du sujet et *sauf mention contraire*, utiliser les connaissances acquises en MPSI.
- L'utilisation de la calculatrice est *autorisée* pour cette épreuve.

**Veuillez ne pas tourner cette page
avant le début de l'épreuve**

On considère dans tout ce problème :

- $\mathbb{K}$, un corps.
- $\mathbb{K}[X]$ est l'anneau des polynômes à une indéterminée définie sur $\mathbb{K}$.
- $\mathbb{K}[X, Y, Z]$ est l'anneau des polynômes à trois indéterminées définie sur $\mathbb{K}$:

$$P \in \mathbb{K}[X, Y, Z] \Leftrightarrow \exists \text{ une famille finie } a_{i,j,k} \in \mathbb{K} \text{ telle que } P(X, Y, Z) = \sum_{i,j,k \in \mathbb{N}} a_{i,j,k} X^i Y^j Z^k.$$

On appelle degré du monôme $a_{i,j,k} X^i Y^j Z^k$ 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 $\mathbb{K}^3 \setminus \{(0, 0, 0)\}$:

$$(x, y, z) \mathcal{R} (x', y', z') \quad \text{si et seulement si} \quad \exists t \in \mathbb{K}^* \text{ tel que } (x, y, z) = t(x', y', z')$$

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 $\mathcal{R}$.

L'ensemble $\mathbb{P}_2(\mathbb{K})$ est 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 :

$$\forall (x, y, z) \in \mathbb{K}^3, P(tx, ty, tz) = t^d P(x, y, z)$$

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 :

$$p(x, y, z) = 0 \text{ où } p = X^3 - Y^2 Z - a_1 X Y Z + a_2 X^2 Z - a_3 Y Z^2 + a_4 X Z^2 + a_6 Z^3.$$

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 $p(X, Y, Z) = X^3 - Y^2Z + XZ^2 + 6Z^3$ 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 $y^2 = x^3 + x + 6$, 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) $\Pi = X^3 + X - 6$ n'admet qu'une unique racine sur $\mathbb{R}$. Étudier les variations de Π et représenter 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 $\mathcal{E}$, une 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 1

Soit $\mathcal{L}$, une 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 à $\mathcal{E}$, 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 à $\mathcal{E}$, 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 $q = p(X, Y, -(aX + bY))$ 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 $\tilde{q}(X) = q(X, 1) \in \mathbb{K}[X]$.

(d) Cas $P_1 \neq P_2$.

Calculer $q(x_1, y_1)$ et $q(x_2, y_2)$. Montrer alors que $\tilde{q}\left(\frac{x_1}{y_1}\right) = \tilde{q}\left(\frac{x_2}{y_2}\right) = 0$.

En déduire que $\tilde{q} = \left(X - \frac{x_1}{y_1}\right) \left(X - \frac{x_2}{y_2}\right) (\lambda X + \mu)$ et montrer que $q(X, Y) = Y^3 \tilde{q}\left(\frac{X}{Y}\right)$.

En déduire la proposition 1 dans le cas de deux points distincts.

(e) Expliquer (efficacement) 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 $-P = (\mathcal{O} * \mathcal{O}) * P$ 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 $(2, -4, 1) + (-3, 6, -1)$ 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.