

Feuille de travaux pratiques N°2

Loi de groupe sur une courbe elliptique et équation de Fermat en degré 3

☞ Vous avez vu en cours qu'une courbe elliptique, c'est-à-dire une courbe projective plane non singulière de degré 3 munie d'un point rationnel, possède une équation de Weierstrass qui en caractéristique différente de 2 et 3 s'écrit $Y^2Z = X^3 + aXZ^2 + bZ^3$ (forme courte). En particulier, cela s'applique à la cubique projective C définie sur \mathbb{Q} par l'équation de Fermat $X^3 + Y^3 = Z^3$ de degré 3, dont on va voir qu'elle est « isomorphe » à la courbe elliptique $E : Y^2Z = X^3 - 432Z^3$.

Une courbe elliptique sous forme de Weierstrass est, à l'exception du point « à l'infini » $O = (0 : 1 : 0)$, entièrement contenue dans le sous-espace affine $U_0 = \{(x : y : 1)\} \subset \mathbb{P}^2$. On y pense donc comme d'une courbe affine (augmentée d'un point) et écrit son équation $y^2 = x^3 + ax + b$.

La loi de groupe, définie géométriquement pour toute courbe elliptique, s'exprime par des formules simples dans le cas d'une forme de Weierstrass. Nous établirons ces formules et nous vérifierons, par le calcul, l'associativité de la loi.

Deux courbes elliptiques isomorphes en tant que courbes ont leurs ensembles de points isomorphes en tant que groupes. Nous déterminerons pour finir la structure de groupe sur les points rationnels de la cubique de Fermat C .

La courbe de Fermat de degré 3

Il s'agit de la cubique projective $C : X^3 + Y^3 = Z^3$ (définie sur \mathbb{Q}).

- 1 Vérifier que le point rationnel $P = (-1 : 1 : 0)$ de C est un point d'inflexion. Exhiber une transformation projective u vérifiant $u(P) = O$ et transformant la tangente en P en la droite à l'infini $Z = 0$. Serait-ce encore possible si P n'était pas un point d'inflexion ? En déduire que C est isomorphe à une courbe d'équation (de Weierstrass longue)

$$ay^2 + bxy + cy = dx^3 + ex^2 + fx + g,$$

où les coefficients sont rationnels (et $a \neq 0, d \neq 0$).

- 2 A l'aide d'un second changement de coordonnées, montrer enfin que C est isomorphe à la courbe elliptique E définie par l'équation de Weierstrass (courte) $y^2 = x^3 - 432$. On explicitera l'isomorphisme.
- 3 Soit C_0 et E_0 les parties affines (dans U_0) de C et E respectivement. Tracer $C_0(\mathbb{R})$ et $E_0(\mathbb{R})$ sur une même figure. Faire de même avec les parties affines C_1 et E_1 dans $U_1 = \{(x : 1 : z)\} \subset \mathbb{P}^2$.

☞ Quelques commandes Maple utiles : `subs`, `diff`, `simplify`, `normal`, `surd`, `plot`, `plots[display]`.

La loi de groupe

On se donne maintenant une courbe elliptique E quelconque donnée par une équation de Weierstrass $y^2 = x^3 + ax + b$ ($a, b \in \mathbb{Q}$ et $\Delta = 4a^3 + 27b^2 \neq 0$). Soit P et Q deux points de E qui, s'ils ne coïncident pas avec O , seront de coordonnées respectives (x_1, y_1) et (x_2, y_2) .

4 En utilisant Maple pour calculer à votre place, démontrer les formules suivantes pour la somme $P + Q$, dont les coordonnées seront notées (x_3, y_3) , lorsque $P + Q \neq O$:

- Cas triviaux : $P + O = P, O + Q = Q, O + O = O$; on suppose désormais $P \neq O$ et $Q \neq O$.
- Si $x_1 \neq x_2$ (i.e. $Q \notin \{P, -P\}$) :

$$(1) \quad \begin{cases} x_3 = \alpha^2 - x_1 - x_2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) \end{cases} \quad \text{où } \alpha = \frac{y_2 - y_1}{x_2 - x_1};$$

- Si $x_1 = x_2$ et $y_1 \neq -y_2$ (i.e. $Q = P$) :

$$(2) \quad \begin{cases} x_3 = \alpha^2 - 2x_1 \\ y_3 = -y_1 + \alpha(x_1 - x_3) \end{cases} \quad \text{où } \alpha = \frac{3x_1^2 + a}{2y_1};$$

- Si $x_1 = x_2$ et $y_1 = -y_2$ (i.e. $Q = -P$) alors $P + Q = O$.

5 Afin d'implémenter la loi de groupe, on définit un point P par la liste $P := [x, y]$ de ses coordonnées si $P \neq O$ et convient de désigner le point à l'infini O par la variable symbolique *Origine*. D'autre part, la courbe elliptique E est définie par le couple $E := [a, b]$.

Ecrire une procédure `appart(E, P)` testant si le point P appartient à E ainsi que deux procédures `somme1(E, P, Q)` et `somme2(E, P)` renvoyant $P + Q$ calculé avec les formules (1) et (2) respectivement. Enfin, écrire une procédure `somme(E, P, Q)` renvoyant *Origine* si $P + Q = O$ et les coordonnées de $P + Q$ sinon (on prendra soin de traiter tous les cas de figure et de procéder au préalable aux vérifications qui s'imposent).

Test : prendre $E : y^2 = x^3 - 36x$, $P = (-3, 9)$ et $Q = (-2, 8)$. Calculer $P + Q$, $2P$ et $2Q$. On doit trouver $(6, 0)$, $(\frac{25}{4}, -\frac{35}{8})$ et $(\frac{25}{4}, \frac{35}{8})$ dans l'ordre. Que remarquez-vous concernant $2P$ et $2Q$?

6 On désire vérifier l'associativité de la loi de groupe ainsi définie et se donne donc trois points P, Q et R de C . A l'aide des procédures `somme1` et `somme2` ainsi que de la procédure de simplification suivante (consultez l'aide afin de comprendre son fonctionnement), démontrer que c'est bien le cas.

```
[> simplifier:=proc(expression)
  local temp, hyp1, hyp2, hyp3;
  hyp1:=P[2]^2=P[1]^3+a*P[1]+b;
  hyp2:=Q[2]^2=Q[1]^3+a*Q[1]+b;
  hyp3:=R[2]^2=R[1]^3+a*R[1]+b;
  temp:=normal(expression, expanded);
  temp:=algsubs(hyp1, temp);
  temp:=algsubs(hyp2, temp);
  temp:=algsubs(hyp3, temp);
  temp:=normal(temp);
  RETURN(temp); end;
```

Remarque. Comprenez-vous maintenant pourquoi une preuve géométrique (basée sur le «théorème de Bezout») est bien plus jolie?

☞ Quelques commandes Maple utiles : `expand`, `collect`, `coeff`.

Application à la cubique de Fermat

On revient à la courbe elliptique $E : y^2 = x^3 - 432$.

- 7** Sachant le théorème de Fermat pour $n = 3$, déterminer $E(\mathbb{Q})$.
- 8** En tant que groupe, caractériser $E(\mathbb{Q})$. Donner un générateur P et vérifier avec la procédure `somme` qu'il engendre bien $E(\mathbb{Q})$.
- 9** *Question subsidiaire* : si E désigne maintenant la courbe de la question 5 utilisée pour tester la procédure `somme`, quelle conjecture faites-vous concernant l'ordre de P et Q dans le groupe $E(\mathbb{Q})$?