

Sous-groupe de 2-torsion des courbes elliptiques en car. 2

Soient k un corps algébriquement clos de caractéristique 2 et E une courbe elliptique sur k . On va calculer explicitement le sous-groupe $E[2]$. Un des avantages du cas $p = 2$ est que pour un point $P \in E$, on a $2P = 0$ ssi $P = -P$. Or on a des formules plus simples pour l'inversion $P \mapsto -P$ que pour la duplication $P \mapsto 2P$. (Voir Silverman chapitre III paragraphe 2 pour les formules explicites de la loi de groupe, qui nous seront utiles).

1 Le schéma affine $E[2]$

On part d'une équation de Weierstrass sous une forme simple. Pour la caractéristique 2, on peut utiliser la forme normale de Deuring (voir Silverman Appendix A) qui est une équation

$$y^2 + \alpha xy + y = x^3 \quad \alpha \in k, \alpha^3 \neq 27.$$

(En car. 2 ceci s'écrit plus simplement $\alpha^3 \neq 1$.) L'invariant j de cette courbe est

$$j = \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27} = \frac{\alpha^{12}}{\alpha^3 + 1}.$$

L'espace topologique sous-jacent au groupe $E[2]$ étant fini, ce groupe est inclus dans un ouvert affine de E . Le problème qui se pose est que la tradition est de prendre une "carte affine" dans laquelle le point O est à l'infini. Ce n'est pas commode pour nous car le sous-groupe $E[2]$ contient O et on veut au contraire une carte affine qui contienne O . Notre première tâche est de trouver une telle carte.

L'équation homogène est

$$y^2z + \alpha xyz + yz^2 = x^3$$

et le point à l'infini est $O = [0 : 1 : 0]$. L'inversion envoie $P = [x : y : z]$ sur $-P = [x : y + \alpha x + z : z]$. Montrons que l'hyperplan projectif d'équation $y = 0$ ne contient pas de point de 2-torsion ; on pourra alors déshomogénéiser en y et obtenir une équation affine qui contient le point O à distance finie. En effet, si un point (fermé) P vérifie $y = 0$, alors en injectant dans l'équation de la courbe on trouve $x = 0$, donc $z \neq 0$. Mais alors on ne peut avoir $[x : y : z] = [x : y + \alpha x + z : z]$.

Donc $E[2]$ est contenu dans le complémentaire du plan $y = 0$, et on peut déshomogénéiser en y (i.e. on fait $y = 1$) pour obtenir la nouvelle équation :

$$z + \alpha xz + z^2 = x^3$$

Cette carte affine contient le point O de coordonnées $x = z = 0$ et tout le sous-groupe $E[2]$. L'inversion est maintenant

$$[x : 1 : z] \mapsto [x : 1 + \alpha x + z : z].$$

On voit facilement avec cette expression que l'équation $P = -P$ n'est pas possible si $1 + \alpha x + z = 0$. Donc pour trouver $E[2]$ on peut travailler dans l'ouvert où $1 + \alpha x + z \neq 0$, c'est-à-dire que techniquement, on peut inverser $1 + \alpha x + z$. Ceci nous permet d'exprimer l'inversion en coordonnées non homogènes (x, z) , précisément si on note $P = (x, z)$ on a

$$-P = \left(\frac{x}{1 + \alpha x + z}, \frac{z}{1 + \alpha x + z} \right).$$

Le sous-groupe $E[2]$, ou plutôt son foncteur de points, est défini par les équations $P = -P$. Ceci se lit $x = \frac{x}{1+\alpha x+z}$ et $z = \frac{z}{1+\alpha x+z}$. Après simplification, on trouve $\alpha x^2 + xz = 0$ et $\alpha xz + z^2 = 0$. L'anneau de fonctions de $E[2]$ est donc le quotient de l'anneau de fonctions de E :

$$\frac{k[x, z]}{(z + \alpha xz + z^2 + x^3)}$$

par les équations $\alpha x^2 + xz = \alpha xz + z^2 = 0$. Finalement c'est

$$R = \frac{k[x, z]}{(z + \alpha xz + z^2 + x^3, \alpha x^2 + xz, \alpha xz + z^2)} = \frac{k[x, z]}{(z + x^3, \alpha x^2 + xz, \alpha xz + z^2)} = \frac{k[x]}{(x^4 + \alpha x^2)}.$$

Cette k -algèbre a pour base $\{1, x, x^2, x^3\}$ comme k -EV. Elle est de dimension 4 sur k , on trouve que l'ordre du groupe $E[2]$ est 4, comme le dit la théorie. En tant que schéma,

$$E[2] = \text{Spec} \left(\frac{k[x]}{(x^4 + \alpha x^2)} \right).$$

2 La loi de groupe

On n'a pour l'instant que la structure de $E[2]$ comme k -schéma affine, pas comme groupe. Il faut trouver les équations de la loi de groupe, ou la comultiplication de l'algèbre de Hopf R . Pour cela on va calculer la loi de groupe en mimant ce que fait Silverman dans le chapitre III, puis on restreindra la loi de groupe obtenue à $E[2]$.

Soient $P_1 = (x_1, z_1)$ et $P_2 = (x_2, z_2)$ deux points de E . La droite passant par P_1 et P_2 (la tangente à E , si $P_1 = P_2$) recoupe la courbe elliptique en un point P_3 tel que $P_1 + P_2 + P_3 = 0$. Pour calculer le point $P_1 + P_2$ il faut ensuite prendre l'opposé de P_3 , mais dans $E[2]$ cette étape sera inutile puisque $P = -P$ dans $E[2]$!

Soit $z = \lambda x + \nu$ l'équation de la droite P_1P_2 , on trouve

$$\lambda = \frac{z_1 + z_2}{x_1 + x_2} \quad \text{et} \quad \nu = \frac{z_1 x_2 + z_2 x_1}{x_1 + x_2}.$$

Soit $F(x, z) = z + \alpha xz + z^2 + x^3 = 0$ l'équation de E . Les points intersection de E et de la droite ont des coordonnées x_i qui sont solution de l'équation

$$F(x, \lambda x + \nu) = \lambda x + \nu + \alpha x(\lambda x + \nu) + (\lambda x + \nu)^2 + x^3 = 0,$$

ce qui veut dire que $F(x, \lambda x + \nu) = c(x - x_1)(x - x_2)(x - x_3)$ pour un certain c . En comparant les coefficients de x^3 on trouve $c = 1$. En comparant les coefficients de x^2 on trouve

$$\alpha \lambda + \lambda^2 = x_1 + x_2 + x_3$$

d'où $x_3 = x_1 + x_2 + \alpha \lambda + \lambda^2$. Comme la coordonnée z a disparu de l'anneau de fonctions de $E[2]$, on n'aura pas besoin de l'expression de z_3 .

On restreint maintenant cette loi de groupe à $E[2]$, c'est-à-dire qu'on injecte dans les calculs les relations $z_1 = x_1^3, x_1^4 + \alpha x_1^2$, etc., et pareil en x_2 . On trouve

$$\lambda = \frac{x_1^3 + x_2^3}{x_1 + x_2} = x_1^2 + x_1 x_2 + x_2^2$$

puis

$$x_3 = x_1 + x_2 + \alpha(x_1^2 + x_1 x_2 + x_2^2) + x_1^4 + x_1^2 x_2^2 + x_2^4 = x_1 + x_2 + \alpha x_1 x_2 + x_1^2 x_2^2.$$

C'est la loi de groupe dans $E[2]$. Si on préfère donner la loi avec l'algèbre de Hopf, c'est

$$x \mapsto 1 \otimes x + x \otimes 1 + \alpha x \otimes x + x^2 \otimes x^2.$$

3 Analyse de $E[2]$

Pour analyser ce schéma en groupes, on va regarder sa suite connexe-étale (lire l'exposé de Tate). Tout schéma en groupes fini G sur un corps possède une suite exacte de schémas en groupes

$$1 \rightarrow G^0 \rightarrow G \rightarrow G^{\text{et}} \rightarrow 1$$

avec G^0 connexe (c'est la composante connexe de l'élément neutre) et G^{et} étale. Notons A l'anneau de fonctions de G , alors l'anneau de fonctions de G^{et} est la plus grande sous-algèbre séparable de A . Si de plus le corps de base est parfait alors $G \rightarrow G^{\text{et}}$ a une section, donc G est produit semi-direct de G^0 par G^{et} . Distinguons deux cas.

3.1 Le cas ordinaire : $\alpha \neq 0$

La plus grande sous-algèbre séparable de $k[x]/(x^2(x^2 + \alpha))$ est engendrée par $y = x^2$ qui est racine du polynôme séparable $y(y + \alpha)$. En d'autres termes le quotient $E[2] \rightarrow E[2]^{\text{et}}$ est donné par le morphisme injectif d'algèbres

$$\begin{array}{ccc} \frac{k[y]}{y(y+\alpha)} & \hookrightarrow & \frac{k[x]}{x^2(x^2+\alpha)} \\ y & \mapsto & x^2 \end{array}$$

Comme $k[y]/(y(y + \alpha)) \simeq k \times k$ en tant que k -algèbres, le groupe $E[2]^{\text{et}}$ d'ordre 2 possède deux points fermés, il est en fait constant i.e. isomorphe à $\mathbb{Z}/2\mathbb{Z}$. De plus k étant algébriquement clos, il est parfait ; vérifions que $E[2]^{\text{et}}$ est un sous-groupe de $E[2]$. Il existe $\beta \in k$ tel que $\alpha = \beta^2$ donc $x^2(x^2 + \alpha) = (x(x + \beta))^2$, de sorte qu'on a un morphisme quotient qui identifie $E[2]^{\text{et}}$ à un sous-groupe de $E[2]$:

$$\begin{array}{ccc} \frac{k[x]}{x^2(x^2+\alpha)} & \rightarrow & \frac{k[t]}{t(t+\beta)} \\ x & \mapsto & t \end{array}$$

Pour finir, identifions $E[2]^0$. L'immersion fermée $E[2]^0 \rightarrow E[2]$ est donné par le quotient :

$$\frac{k[x]}{x^2(x^2 + \alpha)} \rightarrow \frac{k[x]}{x^2}$$

Pour avoir la loi de groupe dans $E[2]^0$ on lit la loi de groupe dans $E[2]$ modulo x^2 et on trouve :

$$x_3 = x_1 + x_2 + \alpha x_1 x_2 .$$

C'est maintenant un exercice de voir que l'application

$$E[2]^0 = \text{Spec}(k[x]/x^2) \longrightarrow \mu_{2,k} = \text{Spec}(k[z]/(z^2 - 1))$$

définie sur les anneaux de fonctions par $z \mapsto 1 + \alpha x$ est un isomorphisme de schémas en groupes. Finalement,

$$E[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mu_2 .$$

Les courbes elliptiques avec ce schéma en groupes de 2-torsion sont dites *ordinaires*.

3.2 Le cas supersingulier : $\alpha = 0$

Dans ce cas $x^4 + \alpha x^2 = x^4$ et

$$R \simeq \frac{k[x]}{x^4}.$$

Le groupe $E[2]$ est connexe. Sa loi de groupe est

$$x_3 = x_1 + x_2 + x_1^2 x_2^2.$$

Cette courbe elliptique est dite *supersingulière* ; il n'y en a qu'une en caractéristique $p = 2$, et pour $p > 0$ quelconque il y a un nombre fini de courbes supersingulières. Le groupe $E[2]$ ne peut pas s'exprimer comme un produit simple comme c'était le cas pour les courbes elliptiques ordinaires. On peut tout de même voir qu'il contient un groupe isomorphe à $\alpha_{2,k}$ défini par l'équation $x^2 = 0$ (noyau du Frobenius).