TD1 - Courbes elliptiques et diviseurs

Exercice 1 (Espace projectif)**.** Soit $\mathbb{F}_q$ un corps fini. Montrer que $\#\mathbb{P}^n(\mathbb{F}_q) = \frac{q^{n+1}-1}{q-1}$ (on pourra poser $\pi\colon \mathbb{F}_q^{n+1} \setminus \{0\} \longrightarrow \mathbb{P}^n(\mathbb{F}_q)$ l'application canonique et montrer que $\forall x \in \mathbb{P}^n(\mathbb{F}_q), \#\pi^{-1}(x) = q-1$).

Exercice 2 (Courbes de Fermat)**.** On considère la courbe de Fermat définie par $C\colon x^n + y^n = z^n$ sur un corps k. On pose $f = X^n + Y^n - Z^n \in k[X,Y,Z]$.

1. Donner une condition nécessaire et suffisante sur k pour que C soit lisse.
2. On suppose que C est lisse. On considère $\overline{k}(C) \simeq \overline{k}(x,y) = \mathrm{Frac}\left(\overline{k}[X,Y]/\langle f(X,Y,1\rangle\right)$ le corps des fonctions rationnelles de C. Montrer que y est une uniformisante de C au point $(1,0)$ dans la carte affine $Z=1$. Quel est l'ordre de $x-1$?

Exercice 3. On considère la courbe elliptique définie par $E\colon y^2 = x^3 + x + 2$ sur $\mathbb{F}_5$.

1. Justifier qu'il s'agit bien d'une courbe elliptique (i.e. que E est lisse).
2. Énumérer les points rationnels de E. Pourquoi peut-on affirmer que le cardinal de $E(\mathbb{F}_{25})$ est un multiple de 4 ? (On ne demande pas de déterminer $E(\mathbb{F}_{25})$).
3. On pose $P = (1,2)$ et $Q = (-1,0)$. Calculer $P+Q$:
   (a) En utilisant la définition.
   (b) Grâce aux formules de somme de deux points.

   En vous appuyant sur ce calcul que vaut $2P$? Quelle est la structure de groupe de $E(\mathbb{F}_5)$?
4. Est-ce que $E(\mathbb{F}_5)$ contient un point non trivial de 3-torsion ? Contient-il un point non-trivial de 2-torsion ? Contient-il toute la 2-torsion ?
5. Calculer $j(E)$.
6. On considère maintenant $E'\colon y^2 = x^3 - x - 1$.
   (a) Montrer que E' a 8 points rationnels.
   (b) Les courbes E et E' sont-elles isomorphes sur $\overline{\mathbb{F}_5}$? Sur $\mathbb{F}_5$?

Exercice 4. Soit $E\colon y^2 = f(x)$ avec $\deg f = 3$ une courbe elliptique sur un corps k. On pose e_1, e_2 et e_3 les trois racines distinctes de f dans $\overline{k}$, $P_i = [e_i\colon 0\colon 1] \in E$ et $O = [0\colon 1\colon 0]$ le point à l'infini. Montrer que
— $\mathrm{div}\, y = [P_1] + [P_2] + [P_3] - 3O$.
— $\mathrm{div}\, x = [R] + [\widetilde{R}] - 2O$ pour un point R que l'on précisera.

Exercice 5 (Critère de principalité)**.** Soit E une courbe elliptique et $D = \sum n_P[P]$ un diviseur de E. Montrer que D est un diviseur principal si, et seulement si,

$$\deg D = 0 \text{ et } \sum n_P P = O$$

(la seconde somme est une somme dans le groupe $(E,+)$). On pourra utiliser l'isomorphisme

$$\begin{array}{rccc} J\colon & E & \longrightarrow & \mathrm{Pic}^0(E) \\ & P & \longmapsto & [P]-[O]. \end{array}$$

Exercice 6 (Modèle de Legendre)**.** Soit $E\colon y^2 = x^3 + ax + b$ une courbe elliptique sur un corps k de caractéristique [1] différente de 2 et 3.

1. Montrer que E est isomorphe à une courbe elliptique donnée par un modèle de Weierstrass du type
$$E'\colon y^2 = x(x-1)(x-\lambda)$$
avec $\lambda \notin \{0,1\}$ (un tel modèle est appelé *modèle de Legendre*, il peut être plus commode dans certaines situations).

1. L'hypothèse $\mathrm{char}\, k \neq 3$ est inutile mais au moment du TD le j-invariant n'a pas encore été défini pour une courbe elliptique quelconque.

2. Montrer que le j-invariant de E est

$$j(E) = 2^8 \frac{\left(\lambda^2 - \lambda + 1\right)^3}{\lambda^2(\lambda - 1)^2}.$$

Exercice 7 (Tordues quadratiques)**.** Soit $E\colon y^2 = x^3 + ax + b$ une courbe elliptique sur un corps k de caractéristique différente de 2 et $d \in k$ qui n'est pas un carré. On pose

$$E^{(d)}\colon y^2 = x^3 + d^2ax + d^3b$$

appelée *tordue* de E par d.

1. Montrer que $E^{(d)}$ est une courbe elliptique.
2. Montrer que $j\left(E^{(d)}\right) = j(E)$. Montrer que $E^{(d)}$ et E sont isomorphes sur $k\left(\sqrt{d}\right)$ mais pas sur k.
3. Montrer que $E^{(d)}$ est isomorphe à la courbe elliptique donnée par $dy^2 = x^3 + ax + b$.
4. On suppose que $E(a, b)$ et $E' = E(a', b')$ sont isomorphes sur $\overline{k}$ et a et b non nuls. Montrer qu'alors E et E' sont isomorphes sur une extension de degré 2 au plus.
   C'est faux en général lorsque a ou b est nul, il se peut que E et E' soient isomorphes sur une extension de degré 4 ou 6.