TD4 : isomorphismes, automorphismes

Exercice 1. 1. Montrer que la courbe d'équation $y^2 = x^3 + B$ possède un automorphisme d'ordre six.

2. Montrer que la courbe d'équation $y^2 = x^3 + Ax$ possède un automorphisme d'ordre quatre.

Exercice 2. Montrer que les courbes $y^2 + y = x^3 + 1$ et $y^2 + y = x^3$ sont isomorphes sur $\mathbb{F}_2$.

Exercice 3. Montrer que sur $\mathbb{F}_2$, toute courbe elliptique est isomorphe à une des cinq courbes suivantes :

$$y^2 + y = x^3 + x + 1, \quad y^2 + y = x^3 + 1, \quad y^2 + y = x^3 + x, \quad y^2 + xy = x^3 + x^2 + 1, \quad y^2 + xy = x^3 + 1$$

Pour chacune de ces courbes, calculer le nombre de points. Y a-t-il une de ces courbes dont le groupe est isomorphe à $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$?

Exercice 4. Classifier les courbes elliptiques sur $\mathbb{F}_3$ (il y en a huit à isomorphisme près). Montrer que tous les ordres dans l'intervalle de Hasse sont réalisés, et que toutes les structures de groupes possibles pour ces cardinaux sont réalisés.

Montrer ensuite qu'il y a douze courbes elliptiques sur $\mathbb{F}_5$, à isomorphisme près. Toutes les structures de groupe dans l'intervalle de Hasse sont-elles possibles ?

Exercice 5. [Forme de Legendre] Une courbe de Legendre est une courbe de la forme

$$L_\lambda : y^2 = x(x-1)(x-\lambda).$$

1. Montrer que toute courbe n'est pas isomorphe à une courbe de Legendre.
2. Montrer que si $\mathrm{car}(k) \neq 2$, toute courbe elliptique sur k est isomorphe sur $\bar{k}$ à une courbe de Legendre (avec $\lambda \in \bar{k}$).
3. Montrer que si on remplace λ par $\frac{1}{\lambda}$, $1-\lambda$, $\frac{\lambda}{\lambda-1}$ ou $\frac{\lambda-1}{\lambda}$, on obtient des courbes isomorphes.

Exercice 6. [Automorphismes en caractéristique trois] Soit k un corps de caractéristique trois. On admet qu'une courbe elliptique sur k est isomorphe à une courbe donnée par une équation de Weiestrass de la forme :

$$y^2 = x^3 + a_2x^2 + a_6 \text{ ou } y^2 = x^3 + a_4x + a_6$$

1. Dans le premier cas, montrer que $\mathrm{Aut}(E)$ est de cardinal deux.
2. Dans le second cas, montrer qu'il est de cardinal douze. (Ce groupe possède un sous-groupe distingué d'ordre trois, c'est un produit semi-direct.)

Exercice 7. [Automorphismes en caractéristique deux, $j \neq 0$] Soit k un corps de caractéristique deux. On considère une courbe elliptique admettant une équation de la forme $y^2 + xy = x^3 + a_2x^2 + a_6$. Montrer que $\mathrm{Aut}(E)$ est de cardinal deux.

Exercice 8. [Automorphismes en caractéristique deux, suite] Soit E la courbe sur $\mathbb{F}_2$ définie par l'équation $y^2 + y = x^3$. Soient $u, s, t \in \overline{\mathbb{F}_2}$ vérifiant $u^3 = 1$, $s^4 + s = 0$ et $t^2 + t = s^6$.

1. Montrer que $(x, y) \mapsto (u^2x + s^2, y + u^2sx + t)$ est un automorphisme de E.
2. Montrer que tout automorphisme de E est de cette forme, et donc qu'il y a 24 automorphismes.
3. Si $\phi \in \mathrm{Aut}(E)$, montrer que $\phi^2 = \pm 1$ ou bien $\phi^3 = \pm 1$.
4. Montrer que $\mathrm{Aut}(E)$ est non-abélien.