Examen Partiel - Courbes Elliptiques

mardi 18 décembre 2012, 9h – 11h

Documents de cours autorisés

Toutes les réponses devront être soigneusement justifiées

Corrigé

Exercice 1.

(1) Montrer que le polynôme $P(X) = X^3 + X^2 + 1$ est irréductible dans $\mathbb{F}_5[X]$. En déduire que $\mathbb{F}_{125} = \mathbb{F}_5(\theta)$ où $\theta^3 + \theta^2 + 1 = 0$.
(2) Calculer θ^{-1} en fonction de θ.
(3) Calculer θ^{30}, puis θ^{31}. En déduire que θ et $-\theta$ sont des carrés dans $\mathbb{F}_{125}$.

On considère la courbe E définie sur $\mathbb{F}_{125}$ d'équation

$$y^2 = x^3 + \theta x.$$

(4) Calculer le discriminant et le j-invariant de E. En déduire que E est une courbe elliptique.
(5) Montrer qu'il existent trois points dans $E(\mathbb{F}_{125})$ de la forme $(x, 0)$. En déduire que $E(\mathbb{F}_{125})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(6) Montrer que les points $P_1 = (\theta, 3)$, $P_2 = (1, 2\theta + 2\theta^2)$ et $P_3 = (-1, \theta + \theta^2)$ sont sur E. Calculer $P_2 + P_3$.

Solution.

(1) $P(X) \neq 0 \mod 5$ pour $X = 0, 1, 2, 3, 4$. Donc P n'a pas de facteur linéaire ; comme il est de degré trois, il est irréductible. Ainsi

$$\mathbb{F}_{125} = \mathbb{F}_{5^3} \cong \mathbb{F}_5[X]/(P) \cong \mathbb{F}(\theta),$$

où $\theta = X + (P) \in \mathbb{F}_5[X]/(P)$ satisfait de $0 = P(\theta) = \theta^3 + \theta^2 + 1$.
(2) On a $\theta(\theta^2 + \theta) = -1$. Donc $\theta^{-1} = -\theta^2 - \theta$.
(3) $\theta^3 = -\theta^2 - 1$, d'où

$$\begin{aligned}\theta^6 = (-\theta^2 - 1)^2 = \theta^4 + 2\theta^2 + 1 = \theta(-\theta^2 - 1) + 2\theta^2 + 1 = -\theta^3 - \theta + 2\theta^2 + 1 \\ = \theta^2 + 1 - \theta + 2\theta^2 + 1 = -2\theta^2 - \theta + 2.\end{aligned}$$

Donc

$$\begin{aligned}\theta^{30} = (\theta^6)^5 = (-2\theta^2 - \theta + 2)^5 = -2(\theta^2)^5 - \theta^5 + 2 = \theta^4(-2\theta^6 - \theta) + 2 \\ = \theta^4(-2(-2\theta^2 - \theta + 2) - \theta) + 2 = -\theta^2 + \theta^5 + \theta^4 + 2 \\ = 2\theta^2 + \theta - 2 + \theta^2(\theta^3 + \theta^2) + 2 = 2\theta^2 + \theta - \theta^2 = \theta^2 + \theta = -\theta^{-1}.\end{aligned}$$

Ainsi $\theta^{31} = -1$. Comme $\mathbb{F}_{125}$ est cyclique d'ordre 124 et $\theta^{62} = 1$, il suit que θ est un carré. Or, $-\theta = 2^2\theta$, donc $-\theta$ est également un carré.
(4) D'après le cours,

$$\Delta(E) = -16(4a_4^3 + 27a_6^2) = \theta^3 \quad \text{et} \quad j(E) = -(48a_4)^3/\Delta = -2.$$

Comme $\Delta(E) \neq 0$, la courbe est lisse et E est une courbe elliptique.
(5) On a $Q_0 = (0, 0) =\in E(\mathbb{F}_{125})$. Si $\alpha \in \mathbb{F}_{125}$ satisfait $\alpha^2 = -\theta$, alors $Q_1 = (\alpha, 0) \in \mathbb{F}_{125}$ et $Q_2 = (-\alpha, 0) \in \mathbb{F}_{125}$, car

$$(\pm\alpha)^3 + (\pm\alpha)\theta = \pm\theta(\alpha^2 + \theta) = 0.$$

Or, $Q_i = -Q_i$ pour $i = 0, 1, 2$. On a donc trois points d'ordre 2 ; comme $|E[2]| = 4$, ce sont tous les points d'ordre deux, et $E(\mathbb{F}_{125})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(6) On a $\theta^3+\theta^2=-1=3^2$; comme $\theta^2(\theta+1)=-1$ on a

$$(2\theta+2\theta^2)^2=4(-\theta^{-1})^2=-\theta^{-2}=\theta+1.$$

Enfin, $(\theta+\theta^2)^2=(-\theta^{-1})^2=-\theta-1$. Ainsi, P_1, P_2 et P_3 sont sur la courbe.

Pour calculer $P_2+P_3=(x,y)$, calculons

$$\lambda=\frac{(2\theta^2+2\theta)-(\theta+\theta^2)}{1-(-1)}=3(\theta+\theta^2)=2\theta^{-1}.$$

Donc $x=\lambda^2-1-(-1)=-\theta^{-2}=\theta+1$ et

$$y=\lambda(1-\theta-1)-(2\theta+2\theta^2)=2\theta^{-1}(-\theta)-2\theta-2\theta^2=-2-2\theta-2\theta^2.$$

Exercice 2. On considère la courbe

$$E: y^2=x^3+\theta x^2+\theta$$

sur le corps $\mathbb{F}_9=\mathbb{F}_3(\theta)$, où $\theta^2=-1$.

(1) Montrer que E est une courbe elliptique; calculer son discriminant et son j-invariant.
(2) Déterminer les points de $E(\mathbb{F}_9)$.
(3) En déduire la valeur t de la trace du Frobenius. La courbe, est-elle supersingulière ?
(4) Le groupe $E(\mathbb{F}_9)$, est-il cyclique ?
(5) Quelle est la plus petite extension k de $\mathbb{F}_9$ tel que $E(k)$ ait un point d'ordre 2 ?

Solution.

(1) D'après le cours,

$$\Delta(E)=-a_2^3a_6=-\theta^4=-1 \quad \text{et} \quad j(E)=-a_2^3/a_6=-\theta^2=1.$$

Comme $\Delta(E)\neq 0$, la courbe est lisse et E est une courbe elliptique.

(2)

x	x^2	x^3	$x^3+\theta x^2+\theta$
0	0	0	θ
1	1	1	$1-\theta$
-1	1	-1	$-1-\theta$
θ	-1	$-\theta$	$-\theta$
$-\theta$	-1	θ	θ
$\theta+1$	$-\theta$	$1-\theta$	-1
$-\theta-1$	$-\theta$	$\theta-1$	$-\theta$
$\theta-1$	θ	$-1-\theta$	1
$1-\theta$	θ	$1+\theta$	$-\theta$

On a donc

$$\begin{aligned}E(\mathbb{F}_9)=\{&O,(0,\theta-1),(0,1-\theta),(\theta,\theta+1),(\theta,-1-\theta),(-\theta,\theta-1),(-\theta,1-\theta),\\&(\theta+1,\theta),(\theta+1,-\theta),(-1-\theta,\theta+1),(-1-\theta,-1-\theta),\\&(\theta-1,1),(\theta-1,-1),(1-\theta,\theta+1),(1-\theta,-1-\theta)\}\end{aligned}$$

et $|E(\mathbb{F}_9)|=15$.

(3) On a $t=9+1-|E(\mathbb{F}_9)|=-5$. Comme $3\nmid -5$, la courbe n'est pas supersingulière.
(4) Comme $15=3\cdot 5$ n'a pas de facteur carré, $E(\mathbb{F}_9)$ est un groupe cyclique.
(5) Un point d'ordre deux est un point de la forme $(x,0)$. Il convient donc de ressoudre $P(x)=x^3+\theta x+\theta=0$. Or, P n'a pas de zéro dans $\mathbb{F}_9$, et donc pas de facteur linéaire. Il est donc irréductible, et la plus petite extension de $\mathbb{F}_9$ tel que P y ait un zéro est $k=\mathbb{F}_{9^3}=\mathbb{F}_9[X]/(P)$.