Feuille d'exercices 7

Avertissement : tous les exercices ne seront pas traités durant les séances ; pour en suivre l'avancement veuillez consulter mon site personnel dans la rubrique *Forum*.

Courbes elliptiques

1. Sur $\mathbb{C}$

Exercice 1. — *Une fonction f est dite* ***elliptique*** *par rapport à un réseau Λ si c'est une fonction méromorphe sur $\mathbb{C}$ qui est Λ-périodique, i.e.*

$$f(z+\omega) = f(z)$$

pour tout $z \in \mathbb{C}$ et tout $\omega \in \Lambda$; c'est bien sûr équivalent à $f(z+\omega_1) = f(z) = f(z+\omega_2)$ pour tout $z \in \mathbb{C}$ avec $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$.

(1) Montrer que si f n'a pas de poles, montrer que f est constante.

(2) Soit f une fonction elliptique par rapport à Λ et soit P un parallélogramme fondamental.

(i) On suppose que f n'a pas de poles sur le bord ∂P de P. Montrer alors que la somme des résidus de f dans P est égale à 0.

(ii) On suppose que f n'a ni zéros ni poles sur ∂P. On note a_i les zéros et poles de f dans P et on note m_i la multiplicité de f en a_i. Montrer que

$$\sum_i m_i = 0$$

$$\sum_i m_i a_i \equiv 0 \mod \Lambda$$

(3) On considère la fonction $\mathfrak{P}$ de Weierstrass :

$$\mathfrak{P}_\Lambda(x) = x^{-2} + \sum_{\omega \in \Lambda - 0} [(x-\omega)^{-2} - \omega^{-2}]$$

(i) Montrer que pour tout $s > 2$ la somme $\sum_{\omega\in\Lambda-0} \frac{1}{|\omega|^s}$ converge. En déduire que la série qui définit $\mathfrak{P}$ converge uniformément sur tout compact de $\mathbb{C}$ ne contenant pas les points du réseau Λ.

(ii) En considérant $\mathfrak{P}'(x) = -2\sum_{x\in\Gamma}(x-\omega)^{-3}$, montrer que $\mathfrak{P}$ est elliptique par rapport à Λ.

(4) L'ensemble des fonctions elliptiques par rapport à Λ est un corps sur $\mathbb{C}$; on veut montrer que celui-ci est engendré par $\mathfrak{P}$ et $\mathfrak{P}'$.

(i) Soit f elliptique paire et soit $u \equiv -u \mod \Lambda$ avec $u \not\equiv 0 \mod \Lambda$. Montrer que $g(z) := \mathfrak{P}(z) - \mathfrak{P}(u)$ a un zéro d'ordre 2. En déduire que f a un zéro d'ordre pair en u. Traitez le cas de $u \equiv 0 \mod \Lambda$ en considérant $g = 1/\mathfrak{P}$.

(ii) Soit $(u_i)_{1\le i\le r}$ un famille de points contenant un représentant de chaque classe $(u, -u) \mod \Lambda$ où f a un pole ou un zéro autre que la classe de Λ. On pose

$$m_i = \mathrm{ord}_{u_i} f \text{ si } 2u_i \not\equiv 0 \mod \Lambda$$

$$m_i = \frac{1}{2}\mathrm{ord}_{u_i} f \text{ si } 2u_i \equiv 0 \mod \Lambda$$

Montrer, en utilisant le théorème de Liouville, que f est égal à une constante fois $\prod_{i=1}^r [\mathfrak{P}(z) - \mathfrak{P}(u_i)]^{m_i}$.

(iii) En déduire que $\mathbb{C}(\mathfrak{P})$ est le corps des fonctions elliptiques paires par rapport à Λ, puis que $\mathbb{C}(\mathfrak{P}, \mathfrak{P}')$ est le corps des fonctions elliptiques par rapport à Λ.

(5) On veut montrer que les points $(\mathfrak{P}(z), \mathfrak{P}'(z))$ appartiennent à une cubique d'équation $y^2 = 4x^3 - g_2 x - g_3$ avec $\Delta = g_2^3 - 27g_3^2 \neq 0$.

(i) Montrer que

$$\mathfrak{P}(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) s_{2n+2}(\Lambda) z^{2n}$$

avec $s_n(\Lambda) = s_n = \sum_{\omega\neq 0} \frac{1}{\omega^m}$.

(ii) En posant $g_2 = 60s_4$ *et* $g_3 = 140s_6$*, montrer que* $(\mathfrak{P}(z), \mathfrak{P}'(z))$ *appartiennent à une cubique d'équation* $y^2 = 4x^3 - g_2x - g_3$.

(iii) On pose $e_1 = \mathfrak{P}(\omega_1/2)$*,* $e_2 = \mathfrak{P}(\omega_2)$ *et* $e_3 = \mathfrak{P}(\frac{\omega_1+\omega_2}{2})$*. Montrer que modulo* Γ*,* $\mathfrak{P}'$ *a trois racines simples à savoir* $\omega_1/2$*,* $\omega_2/2$ *et* $(\omega_1+\omega_2)/2$*. En déduire que*

$$(\mathfrak{P}')^2 = 4(\mathfrak{P} - e_1)(\mathfrak{P} - e_2)(\mathfrak{P} - e_3)$$

avec $\Delta = g_2^3 - 27g_3^2 \neq 0$.

(iv) En déduire que

$$x = \frac{1}{2}\int_{\infty}^{\mathfrak{P}(x)} [(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy \mod \Gamma$$

avec $\omega_1 = \int_{\infty}^{e_1}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy$ *et* $\omega_2 = \int_{e_1}^{e_2}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy$.

(v) Montrer que l'équation $y^2 = x^3 - x$ *correspond au réseau* $\mathbb{Z}^2$ *en utilisant l'égalité*

$$\omega_1 = \int_0^1 (x-x^2)^{-1/2}dx = \int_1^{\infty}(x^3-x)^{-1/2}dx = \omega_2/i$$

que l'on montrer via le changement de variable $x \mapsto 1/x$.

Exercice 2. — ***Loi d'addition*** *Etant donné des nombres complexes* g_2*,* g_3 *on peut se demander s'il existe un réseau pour lequel ce sont les invariants associés comme dans l'exercice précédent. La réponse est oui. On considère la courbe projective* A *d'équation*

$$uy^2 = 4x^3 - g_2xu^2 - g_3u^3$$

de point infini $(0,0,1)$ *qui est l'image des points de* Λ *par l'application* $z \mapsto (1, \mathfrak{P}(z), \mathfrak{P}'(z))$.

(1) Montrer que l'application ci-dessus induit une bijection $\mathbb{C}/\Lambda - 0 \longrightarrow A_{\mathbb{C}} - \{\infty\}$*, où* $A_{\mathbb{C}}$ *désigne les points complexes de la cubique* A.

(2) L'ensemble $\mathbb{C}/\Lambda$ *est naturellement muni d'une structure de groupe ; on veut exprimer celle-ci sur* $A_{\mathbb{C}}$*. Nous allons montrer que si* $P_1 = (1, x_1, y_1)$ *et* $P_2 = (1, x_2, y_2)$ *alors* $P_3 = P_1 + P_2 = (1, x_3, y_3)$ *s'exprime avec des fonctions rationnelles en* x_1, x_2, y_1, y_2*. Géométriquement on procède comme dans la figure (**??**) : la droite* (P_1P_2) *intersecte* $A_{\mathbb{C}}$ *en un troisième point* $Q_3 = -P_3$ *et* P_3 *est le symétrique de* Q_3 *par rapport à l'axe des* x.

(i) Soient $u_1, u_2 \in \mathbb{C} - \Lambda$ *et supposons* $u_1 \not\equiv u_2 \mod \Lambda$*. Soient* $a, b \in \mathbb{C}$ *tels que*

$$\mathfrak{P}'(u_1) = a\mathfrak{P}(u_1) + b$$

$$\mathfrak{P}'(u_2) = a\mathfrak{P}(u_2) + b$$

Montrer que $g(z) = \mathfrak{P}'(z) - a\mathfrak{P}(z) - b$ *a* 3 *zéros comptés avec leur multiplicités. A quelle condition n'a-t-ont que* 2 *zéros distincts ?*

(ii) On suppose que $g(z)$ *a 3 zéros distincts. En notant* u_3 *le troisième, montrer que* $u_3 \equiv -(u_1+u_2) \mod \Lambda$*. En déduire que*

$$x_3 = -x_1 - x_2 + \frac{1}{4}\Big(\frac{y_1-y_2}{x_2-x_2}\Big)^2.$$

Traiter le cas des zéros multiples.

(iii) Pour $u_1 \equiv u_2 \mod \Lambda$ *montrer que*

$$\mathfrak{P}(2u) = -2\mathfrak{P}(u) + \frac{1}{4}\Big(\frac{\mathfrak{P}"(u)}{\mathfrak{P}'(u)}\Big)^2.$$

2. Loi d'addition sur un corps quelconque

Exercice 3. — ***Une introduction à la géométrie algébrique***

(1) En vous appuyant sur la classification des coniques projectives de $\mathbb{P}^2_{\mathbb{R}}$*, montrez qu'une conique non dégénérée* C *non vide de* $\mathbb{P}^2_{\mathbb{R}}$ *est projectivement équivalente à la courbe* $XZ = Y^2$.

Montrez que cette courbe admet un paramétrage par $\mathbb{P}^1_{\mathbb{R}}$ *via l'application qui à* (U, V) *associe* (U^2, UV, V^2)*. Quelle est l'application inverse ?*

(2) ***Cas simples du théorème de Bézout***

(i) Soit

$$F(U,V) = a_d U^d + a_{d-1}U^{d-1}V + \cdots + a_0 V^d$$

un polynôme homogène non nul de degré d en 2 variables à coefficients dans un corps k. On lui associe le polynôme en une variable $f(u) = F(u,1)$ et on définit la multiplicité d'un zéro (u,v) de F dans $\mathbb{P}^1_k$ comme la multiplicité de u/v dans f si $v \neq 0$ et sinon en $(1,0)$ comme l'entier $d - \deg f$.
Montrer que F a au plus d zéros dans $\mathbb{P}^1_k$ comptés avec multiplicités.

(ii) Soit $L \subset \mathbb{P}^2_k$ une droite et $D \subset \mathbb{P}^2_k$ une courbe définie par une équation $G(X,Y,Z) = 0$ où G est un polynôme homogène de degré d en X,Y,Z. On suppose $L \nsubseteq D$. Montrer que le cardinal de $L \cap D$ est inférieur ou égal à d.

(iii) Même hypothèse qu'en (ii) en remplaçant L par une conique non dégénérée C : montrer que le cardinal de $C \cap D$ est inférieur ou égal à $2d$.
Remarque : On peut définir une notion de multiplicité d'une intersection en un point de sorte que les résultats précédents soient vrais en comptant avec multiplicité. En outre si k est algébriquement clos, on a alors égalité. Le théorème de Bézout concerne des courbes C et D de degré n et m : leur intersection est alors nm, en comptant les multiplicités et en travaillant sur un corps algébriquement clos.

(3) ***L'espace des coniques*** *Dans la suite on note $S_d(k)$ l'espace des polynômes homogènes de degré d à coefficients dans k, en les variables X,Y,Z. Etant donnés des points $P_1,\cdots,P_r$ de $\mathbb{P}^2_k$, on notera $S_d(P_1,\cdots,P_n)$ le sous-ensemble de $S_d(k)$ constitué des éléments F qui s'annulent sur les P_i.*

(i) Soient $P_1,\cdots,P_5 \in \mathbb{P}^2_{\mathbb{R}}$ des points distincts tels que 4 quelconques ne sont pas colinéaires. Montrer qu'il existe au plus une conique passant par ces 5 points.

(ii) Soit $n \geq 5$ et soient $P_1,\cdots,P_n$ des points tels que 4 quelconques ne sont jamais colinéaires. Montrer alors que l'ensemble des formes quadratiques qui s'annulent sur ces points est de dimension $6-n$.

(iii) ***Un pinceau de coniques*** *est une famille de la forme*

$$C_{\lambda,\mu} := (\lambda Q_1 + \mu Q_2 = 0)$$

où Q_1 et Q_2 sont des coniques. On suppose que le pinceau possède au moins une conique dégénérée, montrer alors qu'elle en possède au plus 3. En outre si $k = \mathbb{R}$, montrer que le pinceau admet toujours une conique dégénérée.

(4) ***Cubiques : exemples***

(i) On considère la cubique de $\mathbb{R}^2$ définie par l'équation $y^2 = x^3 + x^2$. Donnez en une paramétrisation.

(ii) Même question avec la cubique $y^2 = x^3$.

(iii) Soit k un corps de caractéristique différente de 2 et soit $\lambda \in k$ avec $\lambda \neq 0,1$. Montrer que pour si $f,g \in k(t)$ sont tels que $f^2 = g(g-1)(g-\lambda)$ alors $f,g \in k$. Quelle interprétation en donnez-vous sur la cubique $y^2 = x(x-1)(x-\lambda)$?

(5) ***Cas simples du Nullstellensatz*** *: soit k un corps infini et soit $F \in S_d(k)$ un polynôme homogène de degré d à coefficients dans k en les variables X,Y,Z.*

(i) Soit $L \subset \mathbb{P}^2_k$ une droite. Montrer que si F s'annule sur L alors $F = HF'$ où H est une équation de L et $F' \in S_{d-1}(k)$. En déduire que si $P_1,\cdots,P_n$ sont des points de $\mathbb{P}^2_k$ tels que $P_1,\cdots,P_a \in L$ et $P_{a+1},\cdots,P_n \notin L$ avec $a > d$, alors

$$S_d(P_1,\cdots,P_n) = HS_{d-1}(P_{a+1},\cdots,P_n)$$

(ii) Soit $C \subset \mathbb{P}^2_k$, une conique non dégénérée et non vide. Montrer que si F s'annule sur C alors $F = QF'$ où Q est une équation de C et $F' \in S_{d-2}(k)$. En déduire que si $P_1,\cdots,P_n$ sont des points de $\mathbb{P}^2_k$ tels que $P_1,\cdots,P_a \in C$ et $P_{a+1},\cdots,P_n \notin C$ avec $a > 2d$, alors

$$S_d(P_1,\cdots,P_n) = QS_{d-2}(P_{a+1},\cdots,P_n)$$

(iii) Soient $P_1,\cdots,P_8 \in \mathbb{P}^2_k$ des points distincts tels que 4 quelconques ne sont pas colinéaires et que 7 quelconques ne sont pas sur une conique non dégénérée. Montrer alors que $\dim S_3(P_1,\cdots,P_8) = 2$.
Indication *: on traitera séparément le cas où 3 points quelconques ne sont pas colinéaires et 6 quelconques ne sont pas sur une conique non dégénérée.*

(iv) Soient C_1, C_2 deux coniques dont l'intersection est 9 points distincts. Montrer que toute conique D qui passe par 8 d'entre eux passe aussi par le neuvième.

(6) ***Loi d'addition sur une conique*** *: soit $k \subset \mathbb{C}$ et $C \subset \mathbb{P}^2_k$ une cubique d'équation $F = 0$. On suppose que F est irréductible et que pour tout point $P \in C$, il existe une unique droite $L \subset \mathbb{P}^2_k$ telle que P est un zéro multiple de $F_{|L}$. On fixe un point $O \in C$ et on considère la construction suivante :*

Construction *: (a) Soit $A \in C$ et soit $\bar{A}$ le troisième point d'intersection de C avec la droite OA.*

(b) Pour $A, B \in C$ soit R le troisième point d'intersection de AB avec C et on définit $A + B$ comme étant égal à $\bar{R}$.

On veut montrer que l'on définit ainsi une loi de groupe abélien sur C avec O comme élément neutre.

(i) Montrer que la construction précédente est bien définie.

(ii) Montrer que O est bien un élément neutre et que la loi est commutative.

(iii) Montrer que l'inverse de A est le troisième point d'intersection de $\bar{O}A$ avec C.

(iv) ***Associativité*** *: soient A, B, C trois points de C ; la construction de $(A + B) + C = \bar{S}$ utilise les 4 droite (cf. la figure (**??**)) :*

$$L_1 = ABR, \quad L_2 = RO\bar{R}, \quad L_3 = C\bar{R}S, \quad L_4 = SO\bar{S}$$

La construction de $(B + C) + A = \bar{S}'$ utilise les 4 droites

$$M_1 = BCQ, \quad M_2 = QO\bar{Q}, \quad M_3 = A\bar{Q}S', \quad M_4 = S'O\bar{S}'$$

Il s'agit de prouver $\bar{S} = \bar{S}'$ ou de manière équivalente $S = S'$. On considère les deux cubiques

$$D_1 = L_1 + M_2 + L_3 \qquad D_2 = M_1 + L_2 + M_3$$

de sorte que

$$C \cap D_1 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S\} \qquad C \cap D_2 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S'\}$$

Conclure en supposant les 9 points $\{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S\}$ distincts.

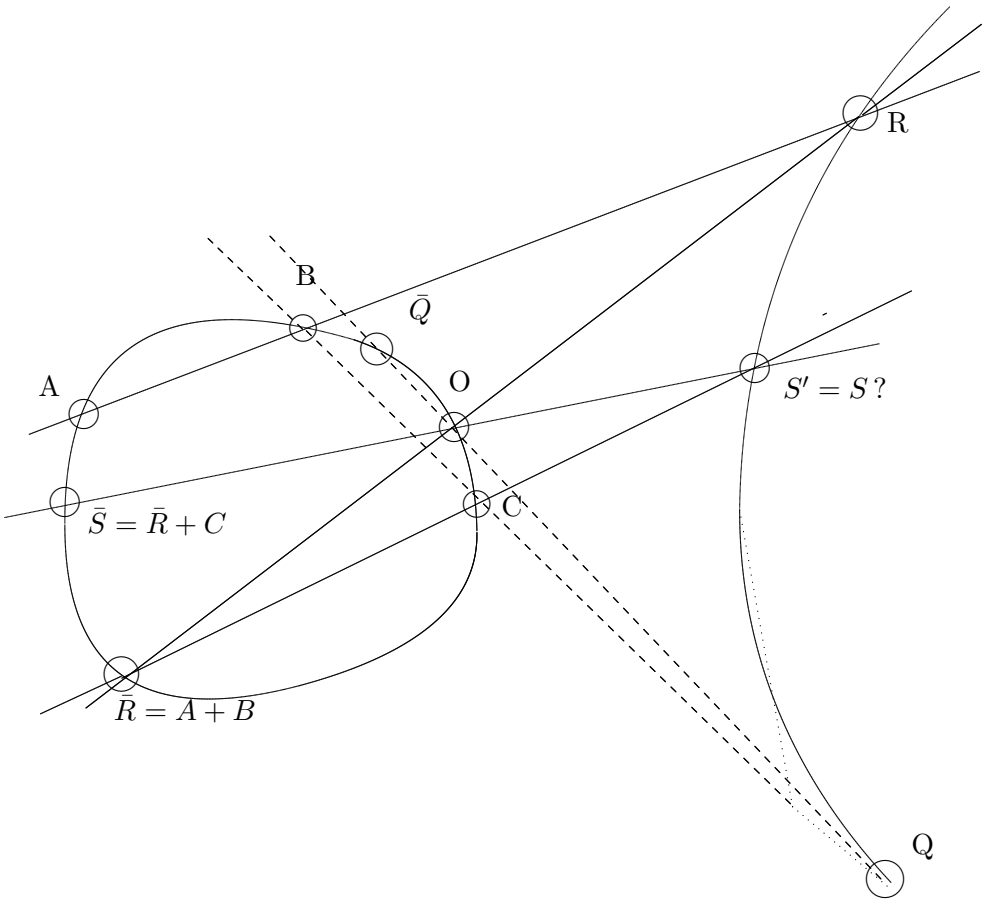

FIGURE 1. Loi d'addition sur une courbe elliptique

(v) Conclure dans le cas général en utilisant un argument de continuité et en utilisant l'hypothèse $k \subset \mathbb{C}$. Remarque : On peut montrer le cas général pour tout k avec une bonne notion de multiplicité, ou bien en utilisant la topologie de Zariski.

(vi) Soit $C \subset \mathbb{P}^2_k$ une cubique possédant un point d'inflexion P. Montrer qu'un changement de coordonnées dans $\mathbb{P}^2_k$ permet de se ramener à une équation de la forme ***normale****, i.e.*

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

Indication *: choisissez les coordonnées telles que $P = (0, 1, 0)$ et la droite d'inflexion $Z = 0$.*

(vii) ***Loi de groupe simplifiée*** *: on considère une cubique sous forme normale et on prend $O = (0, 1, 0)$ comme élément neutre. Montrer que l'on a les propriétés suivantes et retrouver la loi de groupe donnée par les fonctions de Weierstrass.*

(a) $C = \{O\} \cup C_0$, où $C_O : (y^2 = x^3 + ax + b)$ est un courbe affine ;

(b) les droites passant par O sont les droite projectives $X = \lambda Z$ et donc les droites affines $x = \lambda$;

(c) $-P = \bar{P}$.

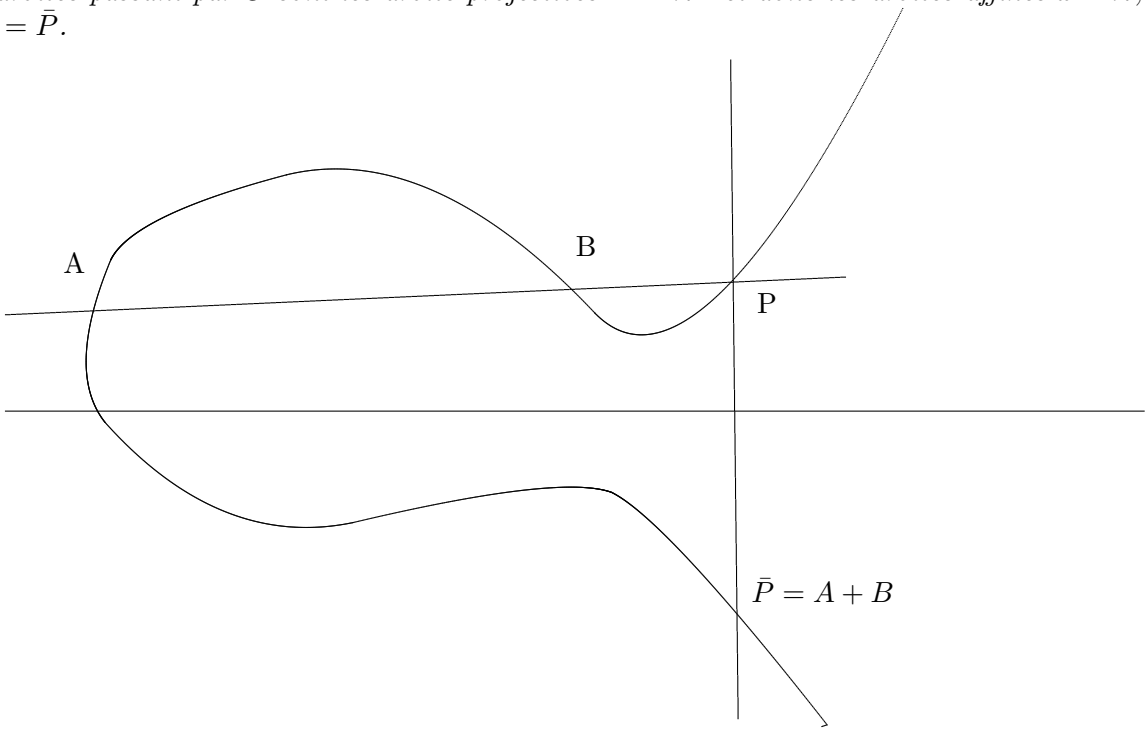

FIGURE 2. Loi d'addition simplifiée

Remarque : Essayez de prouver ***le théorème de l'hexagone de Pascal*** *: Soit un hexagone $ABCDEF$ dans $\mathbb{P}^2_k$ dont les paires de cotés opposés se rencontrent aux points P, Q, R. On suppose les 9 points et les 6 droites distinctes. Montrer alors que*

$$ABCDEF \text{ sont sur une même conique non dégénérée} \Leftrightarrow PQR \text{ sont colinéaires}$$

3. Comptage des points

Exercice 4. — *Soient p un nombre premier ≥ 5 et a un élément non nul de $\mathbb{F}_p$. Soient E et F les cubiques sur $\mathbb{F}_p$ d'équations*

$$E : y^2 = x^3 - ax \quad et \quad F : y^2 = x^3 - a.$$

1. *Montrer que E et F sont des courbes elliptiques définies sur $\mathbb{F}_p$.*
2. *Supposons $p \equiv 3 \mod 4$. Déterminer l'ordre de $E(\mathbb{F}_p)$ (rappelons que l'on tient compte du point à l'infini).*

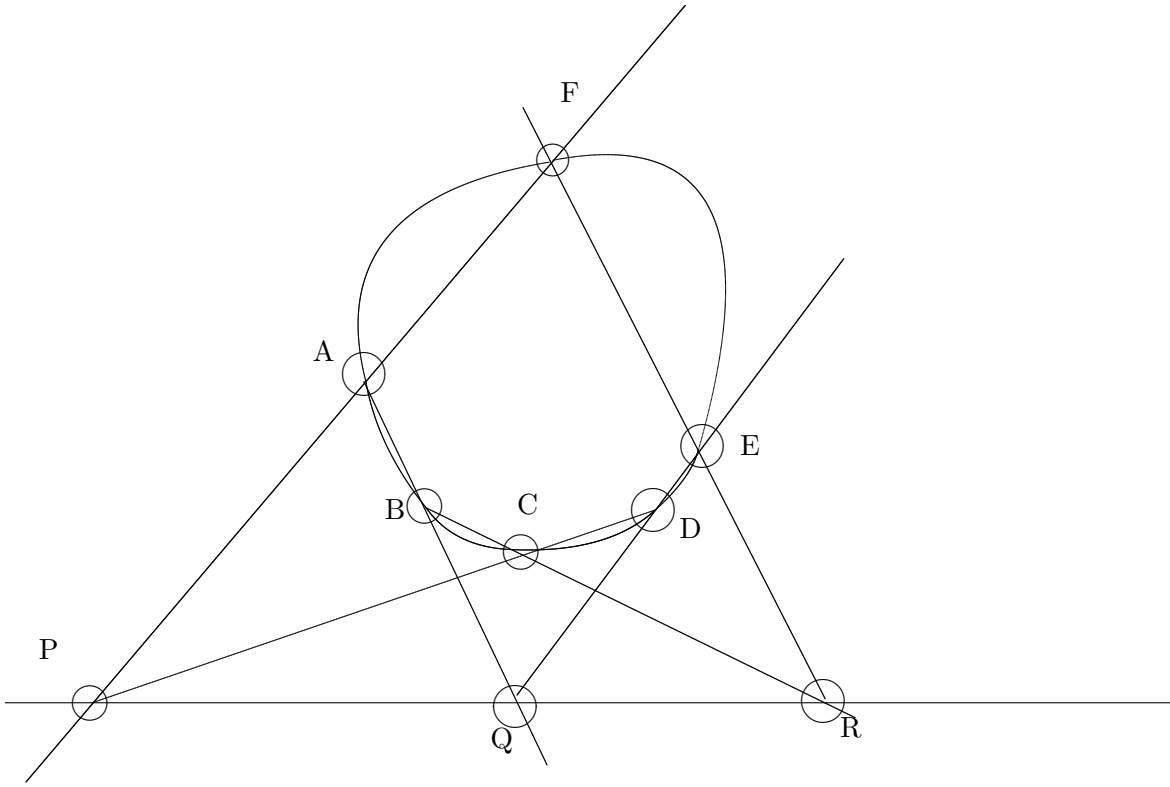

FIGURE 3. L'hexagone de Pascal

3. *Supposons* $p \equiv 2 \mod 3$. *Déterminer l'ordre de* $F(\mathbb{F}_p)$.

Exercice 5. — *Soit* E *la courbe elliptique définie sur* $\mathbb{F}_{31}$ *d'équation*

$$y^2 = x^3 - 3x.$$

1. *Déterminer le sous-groupe des points de* 2*-torsion de* $E(\mathbb{F}_{31})$.
2. *Montrer que le groupe* $E(\mathbb{F}_{31})$ *est cyclique d'ordre* 32. *Déterminer un générateur.*

Exercice 6. — *Soit* E *la cubique sur* $\mathbb{F}_2$ *d'équation*

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

1. *Montrer que* E *est une courbe elliptique sur* $\mathbb{F}_2$.
2. *Soit* $P = (x, y)$ *un point de* E *rationnel sur une extension de* $\mathbb{F}_2$. *Calculer les coordonnées des points* $-P$ *et* $2P$.

   Notons $\mathbb{F}_{16}$ *≪ le ≫ corps de cardinal* 16 *et* $\mathbb{F}_4$ *son sous-corps de cardinal* 4.
3. *Montrer que tout point non nul de* $E(\mathbb{F}_{16})$ *est d'ordre* 3.
4. *Montrer que l'on a* $E(\mathbb{F}_{16}) = E(\mathbb{F}_4)$.
5. *En déduire l'ordre de* $E(\mathbb{F}_4)$ *en utilisant le théorème de Hasse.*

Exercice 7. — *Décrivez le groupe des points sur* $\mathbb{F}_{71}$ *de la courbe elliptique* $y^2 = x^3 - x$.

Exercice 8. — *Soient* K *un corps fini de cardinal* q *et* E *une courbe elliptique définie sur* K. *Montrer qu'il existe un unique couple d'entiers naturels* (d_1, d_2) *tel que* $E(K)$ *soit isomorphe au groupe produit* $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ *et que* d_1 *divise* d_2 *et* d_1 *divise* $q - 1$. *Indication : on admettra les assertions suivantes. Soient* $\overline{K}$ *une clôture algébrique de* K *et* ℓ *la caractéristique de* K. *Pour tout entier* $n \geq 1$, *soit* $E[n]$ *le sous-groupe de* $E\big(\overline{K}\big)$ *formé des points annulés par* n. *Si* ℓ *ne divise pas* n, *le groupe* $E[n]$ *est isomorphe à* $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. *Le groupe* $E[\ell]$ *est trivial ou bien est d'ordre* ℓ. *Par ailleurs, si* n *est un entier non divisible par* ℓ *et si* $E[n]$ *est contenu dans* $E(K)$, *alors le sous-groupe des racines* n*-ièmes de l'unité de* $\overline{K}^*$ *est contenu dans* K.

Exercice 9. — *Soit q une puissance d'un nombre premier p et $\mathbb{F}_q$ $\ll$ le $\gg$ corps fini de cardinal q. Soit $\mathbb{F}_{q^r}$ l'extension de degré r de $\mathbb{F}_q$ contenue dans une clôtute algébrique de $\mathbb{F}_q$ fixée. Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Notons N_r l'ordre du groupe $E\big(\mathbb{F}_{q^r}\big)$ des points de E rationnels sur $\mathbb{F}_{q^r}$. On admettra dans cet exercice qu'il existe deux nombres complexes conjugués l'un de l'autre α et β, de module $\sqrt{q}$, tels que l'on ait*

$$N_r = q^r + 1 - \big(\alpha^r + \beta^r\big) \quad \textit{pour tout } r \geq 1, \tag{1}$$

$$1 - aT + qT^2 = (1-\alpha T)(1-\beta T) \in \mathbb{Z}[T] \quad \textit{avec} \quad a = q + 1 - N_1. \tag{2}$$

On dit que a est la trace du Frobenius de E.

1. *Si l'on a $q = p$ et $p \geq 5$, montrer que pour tout $r \geq 2$, l'entier N_r n'est pas premier.*
2. *Supposons $q = p = 2$. On prend pour E la courbe elliptique sur $\mathbb{F}_2$ d'équation*
$$y^2 + y = x^3 + x + 1.$$
   (a) *Montrer qu'il existe des entiers $r \geq 2$ tels que N_r soit premier.*
   (b) *Supposons r impair. Montrer que l'on a*
$$N_r = 2^r + 1 - \Big(\frac{2}{r}\Big) 2^{\frac{r+1}{2}},$$
   où $\left(\frac{2}{r}\right)$ désigne le symbole de Jacobi.
   (c) *Soit i une racine carrée de -1. Montrer l'énoncé suivant :*
   Lemme Supposons r impair. Les conditions suivantes sont équivalentes :
   (i) l'entier N_r est premier.
   (ii) L'entier $2^r + 1 - \left(\frac{2}{r}\right) 2^{\frac{r+1}{2}}$ est premier.
   (iii) L'élément $(1+i)^r - 1 \in \mathbb{Z}[i]$ est irréductible.
   Si tel est le cas, r est premier.
   (d) *Supposons r pair. Montrer que l'on a*
$$N_r = \begin{cases} \big(2^{\frac{r}{2}} - 1\big)^2 & \textit{si } r \equiv 0 \mod 8 \\ 2^r + 1 & \textit{si } r \equiv 2, 6 \mod 8 \\ \big(2^{\frac{r}{2}} + 1\big)^2 & \textit{si } r \equiv 4 \mod 8 \end{cases}$$
   En déduire que N_r est premier si et seulement si $r = 2$.

Exercice 10. — *On utilisera de nouveau le résultat admis au début de l'énoncé de l'exercice précédent. Soient u un élément de $\mathbb{F}_4$ qui ne soit pas dans $\mathbb{F}_2$ et E la courbe elliptique sur $\mathbb{F}_4$ d'équation*

$$y^2 + y = x^3 + u.$$

1. *Montrer que pour tout $r \geq 1$, l'ordre du groupe $E\big(\mathbb{F}_{4^r}\big)$ est $(2^r - 1)^2$.*
2. *Trouver une formule simple de duplication sur E.*
3. *Soit $r \geq 1$ un entier tel que $2^r - 1$ soit premier. Montrer que les points de $E\big(\mathbb{F}_{4^r}\big)$, autres que le point à l'infini, sont d'ordre $2^r - 1$. En déduire que l'on a un isomorphisme*
$$E\big(\mathbb{F}_{4^r}\big) \simeq \mathbb{Z}/(2^r - 1)\mathbb{Z} \times \mathbb{Z}/(2^r - 1)\mathbb{Z}.$$

4. Solutions

1 (1) Si f n'a pas de pôles, elle est alors bornée sur le compact $\mathbb{C}/\Lambda$ et donc par périodicité sur $\mathbb{C}$. Le théorème de Liouville donne alors que f est constante.

(2) (i) On a

$$2i\pi \sum \mathrm{Res} f = \int_{\partial P} f(z)dz$$

qui est nul par périodicité de f.

(ii) Comme f est elliptique, on en déduit que f' et f/f' le sont aussi. On a alors comme précédemment

$$0 = \int_{\partial P} \frac{f'}{f}(z)dz = 2o\pi \sum m_i$$

Pour la deuxième égalité on utilise

$$\int_{\partial P} z\frac{f'(z)}{f(z)}dz = 2i\pi \sum m_i a_i$$

car $\mathrm{Res}_{a_i} z\frac{f'(z)}{f(z)} = m_i a_i$. En effectuant le changement de variable $u = z - \omega_2$ dans la deuxième intégrale du membre de gauche ci-dessous, on obtient

$$\int_{\alpha}^{\alpha+\omega_1} z\frac{f'(z)}{f(z)}dz - \int_{\alpha+\omega_2}^{\alpha+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz = -\omega_2 \int_{\alpha}^{\alpha+\omega_1} z\frac{f'(z)}{f(z)}dz = 2i\pi k\omega_2$$

pour $k \in \mathbb{N}$. On fait de même pour les deux autres cotés opposés, d'où le résultat.

(3) (i) La somme partielle pour $|\omega| \leq N$ peut se décomposer en une somme sur les anneaux $n-1 \leq |\omega| < n$, pour $1 \leq n \leq N$. Sur chaque anneau, le nombre de points du réseau est d'ordre n et donc

$$\sum_{|\omega|\leq N} \frac{1}{|\omega|^s} \leq \sum_{1}^{\infty} \frac{n}{n^s}$$

qui converge donc pour $s > 2$.

(ii) Par convergence uniforme sur tout compact, on a

$$\mathfrak{P}'(x) = -2\sum_{\omega\in\Lambda} \frac{1}{(x-\omega)^3}$$

qui est donc Λ-périodique et impaire. Ainsi on a

$$\mathfrak{P}(x+\omega_1) = \mathfrak{P}(x) + C$$

et en prenant $x = -\omega_1/2$, qui n'est pas un pôle de $\mathfrak{P}$, on obtient $C = 0$ car $\mathfrak{P}$ est paire. On procède de même pour ω_2 et donc $\mathfrak{P}$ est Λ-périodique.

(4) (i) On a $2u \equiv 0 \mod \Lambda$ ce qui donne dans P, $0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$. Si f est elliptique paire et s'annule en u, on a alors $f'(u) = -f'(-u)$ et donc $f'(u) = 0$, i.e. f a un zéro d'ordre au moins 2 en u. Ainsi si $u \not\equiv 0 \mod \Lambda$, l'argument précédent montre que $g(z)$ a un zéro d'ordre au moins 2 en u et donc exactement d'ordre 2 d'après (ii) car $\mathfrak{P}$ a exactement un pôle d'ordre 2 dans P. Ainsi f/g est paire, elliptique, holomorphe en u. Si $f(u)/g(u) \neq 0$ alors $\mathrm{ord}_u f = 2$ et sinon, on répète l'argument.

Dans le cas où $u \equiv 0 \mod \Lambda$, on utilise $g = 1/\mathfrak{P}$ et on utilise les mêmes arguments.

(ii) D'après ce qui précède, pour $a \not\equiv 0 \mod \Lambda$, la fonction $\mathfrak{P}(z) - \mathfrak{P}(a)$ a un pôle d'ordre 2 en a si et seulement si $2a \equiv 0 \mod \Lambda$ et a deux zéros distincts d'ordre 1 en a et $-a$ sinon. Ainsi pour tout $z \not\equiv 0 \mod \Lambda$,

$$\prod_{i=1}^{r} (\mathfrak{P}(z) - \mathfrak{P}(u_i))^{m_i}$$

a le même ordre en z que f. C'est aussi vrai à l'origine d'après la première égalité de (2) (ii), le résultat découle alors du théorème de Liouville.

(iii) On en déduit donc que $\mathbb{C}(\mathfrak{P})$ est le cors des fonctions elliptiques paires par rapport à Λ. Par ailleurs si f est elliptique, elle s'écrit $f_+ + f_-$ avec f_+ paire et f_- impair. Pour f impair, le produit $f\mathfrak{P}'$ est pair et appartient donc à $\mathbb{C}(\mathfrak{P})$, d'où le résultat.

(5) (i) On écrit

$$\begin{aligned}\mathfrak{P}(z) &= \tfrac{1}{z^2} + \textstyle\sum_{\omega\in\Lambda'}\Big[\tfrac{1}{\omega^2}\big(1+\tfrac{z}{\omega}+(\tfrac{z}{\omega})^2+\cdots\big)^2-\tfrac{1}{\omega^2}\Big]\\ &= \tfrac{1}{z^2} + \textstyle\sum_{\omega\in L'}\sum_{m=1}^{\infty}(m+1)(\tfrac{z}{\omega})^m\tfrac{1}{\omega^2}\\ &= \tfrac{1}{z^2} + \textstyle\sum_{m=1}^{\infty} c_m z^m\end{aligned}$$

avec $c_m = \sum_{\omega\neq 0}\frac{m+1}{\omega^{m+2}}$.

(ii) Ainsi on a

$$\mathfrak{P}(z) = \frac{1}{z^2} + 3s_4z^2 + 5s_6z^4 + \cdots \qquad \mathfrak{P}'(z) = \frac{-2}{z^3} + 6s_4z + 20s_6z^3 + \cdots$$

de sorte que $\phi(z) = \mathfrak{P}'(z)^2 - 4\mathfrak{P}(z)^3 + g_2\mathfrak{P}(z) + g_3$ est une fonction elliptique sans pôle et avec un zéro à l'origine ; elle est donc identiquement nulle.

(iii) La fonction $h(z) = \mathfrak{P}(z) - e_i$ a un zéro en $\omega_i/2$ d'ordre pair, cf. ci-avant, de sorte que $\mathfrak{P}'(\omega_i/2) = 0$. La fonction elliptique $\mathfrak{P}$ prend la valeur e_i avec multiplicité 2 et n'a qu'un pôle d'ordre 2 modulo Λ de sorte que $e_i \neq e_j$ pour $i \neq j$. En comparant les zéros et les pôles, on en déduit donc que

$$(\mathfrak{P}')^2 = 4(\mathfrak{P}-e_1)(\mathfrak{P}-e_2)(\mathfrak{P}-e_3)$$

avec $\Delta \neq 0$.

(iv) De l'équation différentielle

$$dx = d\mathfrak{P}/d\mathfrak{P}' = \frac{1}{2}[(\mathfrak{P}-e_1)(\mathfrak{P}-e_2)(\mathfrak{P}-e_3)]^{-1/2}d\mathfrak{P}$$

on en déduit que

$$x = \frac{1}{2}\int_{\infty}^{\mathfrak{P}(x)}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy \mod \Gamma$$

et donc en particulier $\omega_1 = \int_{\infty}^{e_1}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy$ et $\omega_2 = \int_{e_1}^{e_2}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy$.

(v) On a $x^3 - x = x(x-1)(x+1)$ et donc

$$\omega_1 = \int_0^1 (x-x^3)^{-1/2}dx = \int_1^{\infty}(x^3-x)^{-1/2}dx = \omega_2/i$$

ce qui correspond donc au réseau $\mathbb{Z}_2$.

2 (1) Pour tout nombre complexe α, $\mathfrak{P}(z) - \alpha$ a au plus deux zéros et au moins un, d'où la surjectivité. D'après ce qui précède, le zéro z_1 est simple si $2z_1 \not\equiv 0 \mod \Lambda$ et double sinon. Dans le premier cas, l'autre zéro est $-z_1$ avec $\mathfrak{P}'(-z_1) = -\mathfrak{P}'(z_1) \neq 0$, d'où l'injectivité.

(2) (i) $g(z)$ a un pôle d'ordre 3 en zéro et donc possède 3 zéros comptés avec multiplicités, dont u_1 et u_2. Si u_1 est double, on a alors d'après l'exercice précédent (2) (ii)

$$2u_1 + u_2 \equiv 0 \mod \Lambda$$

de sorte que pour u_1 fixé, il n'y a qu'un nombre fini de valeurs pour u_2.

(ii) L'égalité $u_3 \equiv -u_1 - u_2 \mod \Lambda$ découle de l'exercice précédent (2) (ii). L'équation $4x^3 - g_2x - g_3 - (ax+b)^2 = 0$ a trois racines comptés avec multiplicité, à savoir $\mathfrak{P}(u_1), \mathfrak{P}(u_2), \mathfrak{P}(u_3)$. Les relations coefficients racines donnet

$$\mathfrak{P}(u_1) + \mathfrak{P}(u_2) + \mathfrak{P}(u_3) = \frac{a^2}{4}$$

avec $a = \frac{\mathfrak{P}'(u_1)-\mathfrak{P}'(u_2)}{\mathfrak{P}(u_1)-\mathfrak{P}(u_2)}$ ce qui donne

$$\mathfrak{P}(u_1+u_2) = -\mathfrak{P}(u_1) - \mathfrak{P}(u_2) + \frac{1}{4}\Big(\frac{\mathfrak{P}'(u_1)-\mathfrak{P}'(u_2)}{\mathfrak{P}(u_1)-\mathfrak{P}(u_2)}\Big)^2$$

d'où le résultat. Cette formule est vraie pour tous les $u_2 \not\equiv u_1 \mod \Lambda$ sauf un nombre fini ; c'est donc vrai pour tout $u_2 \not\equiv u_1 \mod \Lambda$ par prolongement analytique.

(iii) La formule s'obtient à partir de la précédente en passant à la limite $u_1 \to u_2$.

3 (1) Les coniques projectives de $\mathbb{P}^2_{\mathbb{R}}$ sont en bijection avec les classes de similitudes des formes matrices symétriques de $\mathbb{M}_3(\mathbb{R})$ via l'action de $GL_3(\mathbb{R})$, où $A \in GL_3(\mathbb{R})$ agit sur M par ${}^tAMA$. Ces classes d'équivalence sont alors déterminées par la signature $(r, s$ avec $r \geq s$. Si on veut la conique non dégénérée il faut en plus que $r + s = 3$, ce qui laisse les couples $(3, 0)$ et $(2, 1)$. Le premier donne une conique vide et la deuxième la conique $U^2 = V^2 - W^2$ qui après le changement de variable $Y = U$, $X = V - W$ et $Z = V + W$ s'écrit $Y^2 = XZ$. En affine la parabole $y^2 = x$ se paramètre par y ce qui donne le paramétrage projectif de l'énoncé. L'application inverse est $(X, Y, Z) \in \mathbb{P}^2_{\mathbb{R}} \mapsto (X, Y) \in \mathbb{P}^1_{\mathbb{R}}$.

(2) (i) Soit m_∞ la multiplicité du zéro de F en $(1, 0)$; par définition $d - m_\infty$ est le degré de polynôme f qui a donc au plus $d - m_\infty$ racines.

Remarque : si k est algébriquement clos, on a évidemment égalité.

(ii) On paramètrise la droite L sous la forme

$$X = a(U, V), \quad Y = b(U, V), \quad Z = c(U, V)$$

où a, b, c sont des formes linéaires en U, V. L'intersection de L avec D est donnée par les $(U, V) \in \mathbb{P}^1_k$ tels que $F(U, V) = G(a(U, V), b(U, V), c(U, V)) = 0$, d'où le résultat d'après la question précédente.

(iii) On paramétrise la conique C sous la forme

$$X = a(U, V), \quad Y = b(U, V), \quad Z = c(U, V)$$

où a, b, c sont des formes quadratiques en U, V ; en effet C est projectivement équivalente à $Y^2 = XY$ paramétrée par (U^2, UV, V^2), i.e.

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = M \begin{pmatrix} U^2 \\ UV \\ V^2 \end{pmatrix}$$

où $M \in GL_3(k)$. Il faut alors résoudre l'équation $F(U, V) = G(a(U, V), b(U, V), c(U, V)) = 0$, d'où le résultat d'après la question précédente.

(3) (i) Soient $C_1 \neq C_2$ deux coniques passant par $P_1, \cdots, P_5$; C_1 est donc non vide et non dégénérée et donc projectivement équivalente à $\{(U^2, UV, V^2) \ / \ (U, V) \in \mathbb{P}^1\}$. D'après la question précédente, on a $C_1 \subset C_2$ de sorte que si Q_2 est une équation de C_2, alors $Q(U^2, UV, V^2) = 0$ pour tout $(U, V) \in \mathbb{P}^1$ et donc Q_2 est un multiple de $XZ - Y^2$ ce qui contredit l'hypothèse $C_1 \neq C_2$.

(ii) $S_2(k)$ est en bijection avec les matrices symétriques de $\mathbb{M}_3(k)$, c'est donc un k-espace vectoriel de dimension 6. Le sous-ensemble des F qui s'annulent en P est le noyau d'une forme linéaire, i.e. un hyperplan, d'où le résultat.

(iii) La conique $C_{\lambda,\mu}$ est dégénérée si et seulement si $\det(\lambda Q_1 + \mu Q_2) = 0$ ce qui donne une équation $F(\lambda, \mu)$ homogène de degré 3 en λ et μ, d'où le résultat.

(4) (i) Le point $(0, 0)$ est clairement un point double. On considère les droite passant par $(0, 0)$ de pente t qui doit couper la cubique en un unique autre point. On obtient alors une paramétrisation $t \mapsto (t^2 - 1, t^3 - 1)$.

(ii) On procède de même ce qui donne $t \mapsto (t^2, t^3)$.

(iii) On rappelle que l'anneau $k[t]$ est principal et donc factoriel. On écrit $f = r/s$ et $g = p/q$ avec r, s et p, q dans $k[t]$ premiers entre eux. On obtient alors

$$r^2 q^3 = s^2 p(p - q)(p - \lambda q)$$

On obtient alors que s^2 divise q^3 et q^3 divise s^2 de sorte que $s^2 = aq^3$ avec $a \in k$. Ainsi $aq = (s/q)^2$ est un carré et de $r^2 = ap(p - q)(p - \lambda q)$ on en déduit qu'il existe des constantes b, c, d tels que bp, $c(p - q)$ et $d(p - \lambda q)$ aussi. Passons dans $\bar{k}[t]$, de sorte que $q = u^2$ et $p = v^2$ avec $p - q = (u - v)(u + v)$ et $p - \lambda q = (u - \alpha v)(u + \alpha v)$ des carrés avec $\alpha^2 = \lambda$. Comme u et v sont premiers entre eux, on en déduit que $u - v$, $u + v$, $u + \alpha v$ et $u - \alpha v$) sont aussi des carrés. On conclut alors par un argument de descente à la Fermat sur le degré des polynômes.

Ainsi la cubique $y^2 = x(x - 1)(x - \lambda)$ n'a pas de paramétrisation rationnelle.

(5) (i) Quitte à faire un changement de coordonnées on suppose que $L = X$ Pour $F \in S_d$, on l'écrit sous la forme $F = X\tilde{F} + G(Y, Z)$ de sorte que G est nulle sur X Or si G était non nul il aurait d'après ce qui précède au plus $d - 1$ zéros sur la droite L d'où la contradiction car k est infini.

Ainsi si F est homogène de degré d et si la courbe $D : (F = 0)$ rencontre L aux points $P_1, \cdots, P_a$ avec $a > d$, alors $L \subset D$ et donc $F = H\tilde{F}$. Comme $P_{a+1}, \cdots, P_n \notin L$ alors $\tilde{F} \in S_{d-1}(P_{a+1}, \cdots, P_n)$.

(ii) Quitte à faire un changement de coordonnées on suppose que $Q = XZ - Y^2$. Pour $F \in S_d$, on l'écrit sous la forme $F = Q\tilde{F} + A(X, Z) + YB(X, Y)$: en effet on substitue à chaque Y^2, $XZ - Q$ de sorte que modulo Q, on

obtient $A(X,Z)+YB(X,Z)$. On paramétrise alors C par (U^2,UV,V^2) de sorte que $A(U^2,V^2)+UVB(U^2,V^2)=0$ sur C. Comme précédemment, k étant infini, on en déduit que $A(U^2,V^2)+UVB(U^2,V^2)=0$ dans $k[U,V]$ ce qui en séparant les parties paires et impaires donne $A(X,Z)=B(X,Z)=0$. Le reste du raisonnement procède comme dans la question précédente.

(iii) Supposons d'abord que 3 points quelconques ne sont pas colinéaires et que 6 quelconques ne sont pas sur une même conique. Supposons par l'absurde que $\dim S_3(P_1,\cdots,P_8)\geq 3$ et soient P_9,P_{10} des points distincts sur la droite P_1P_2. On a alors

$$\dim S_3(P_1,\cdots,P_{10})\geq \dim S_3(P_1,\cdots,P_8)-2\geq 1$$

de sorte qu'il existe $F\neq 0$ dans $S_3(P_1,\cdots,P_{10})$. On en déduit donc d'après (i) que $F=HQ$ avec $Q\in S_2(P_3,\cdots,P_8)$ d'où la contradiction car les 6 points $P_3,\cdots,P_8$ n'appartiennent pas à une même conique d'après l'hypothèse.

Supposons désormais que P_1,P_2,P_3 sont colinéaires, sur la droite L d'équation $H=0$. Soit P_9 un quatrième point sur L. D'après (i) on a

$$S_3(P_1,\cdots,P_9)=HS_2(P_4,\cdots,P_8)$$

Comme 4 quelconques des $P_4,\cdots,P_8$ ne sont colinéaires alors $\dim S_2(P_4,\cdots,P_8)=1$ et donc $\dim S_3(P_1,\cdots,P_9)=1$ ce qui implique $\dim S_3(P_1,\cdots,P_8)\leq 2$.

Supposons enfin que $P_1,\cdots,P_6$ appartiennent à une même conique C d'équation $Q=0$. Soit $P_9\in C$ distincts de $P_1,\cdots,P_6$. D'après (ii), on a

$$S_3(P_1,\cdots,P_9)=QS_1(P_7,P_8)$$

La droite $L=P_7P_8$ est unique de sorte que $S_3(P_1,\cdots,P_9)$ est de dimension 1 et donc $\dim S_3(P_1,\cdots,P_8)\leq 2$.

(iv) Si 4 quelconques parmi $P_1,\cdots,P_9$ sont sur une droite L alors C_1 et C_2 qui rencontrent L en plus de 4 points, la contiennent ce qui n'est pas par hypothèse. Pour les mêmes raisons 7 points quelconques ne sont pas sur une même conique. On en déduit alors que

$$\dim S_3(P_1,\cdots,P_8)=2$$

ce qui signifie que les équations F_1,F_2 de C_1 et C_2 forment une base de $S_3(P_1,\cdots,P_8)$ de sorte que $D=(G=0)$ est de la forme $G=\lambda F_1+\mu F_2$ et passe donc par P_9.

(6) (i) Si P et Q sont distincts alors la droite PQ est unique et bien définie : si $P=Q$ cela découle de l'hypothèse. L'équation $F_{|L}$ est de degré 3 et possède donc 2 zéros et donc un troisième car la somme des racines dans $\mathbb{C}$ est le coefficient sur x^2 et appartient donc à k.

(ii) La construction $O+A$ consiste à prendre la droite OA, puis le troisième point d'intersection $\bar{A}$ puis à reprendre la droite $O\bar{A}=OA$ et prendre le troisième point d'intersection qui est donc A. La commutativité est évidente.

(iii) On considère la droite qui possède O comme point double et soit $\bar{O}$ le troisième point d'intersection. On vérifie alors aisément que le troisième point d'intersection de $\bar{O}A$ avec C est l'inverse de A.

(iv) On utilise la question précédente : C et D_1 vérifient bien les hypothèses de sorte que D_2 doit passer par S et la seule possibilité est $S'=S$.

(v) Il suffit de remarquer que $A+B$ est une fonction continue en A et B et que quitte à bouger un tout petit peu A,B,C en A',B',C', on peut se ramener au cas où les neuf points précédents sont distincts.

(vi) Quitte à effectuer un changement de coordonnées on suppose que le point d'inflexion est $P=(0,1,0)$ et la tangente est $Z=0$. Le fait que $P\in C$ impose qu'il n'y a pas de terme en Y^3. Le fait que $L:(Z=0)$ soit une tangente d'inflexion en P signifie que $f_{|L}$ a un zéro d'ordre 3 en P, i.e. de la forme $ax^3+bx^2z+x(cz^2+c'z)+dz^3+d'z^2+d"z$ soit $f=aX^3+bX^2Z+X(cZ^2+c'ZY)+dZ^3+d'Z^2Y+d"ZY^2$ que l'on peut écrire sous la forme demandée via un égalité du genre $Y^2Z+ZY(\alpha X+\beta Z)=ZY'+aX^2+bXZ+cZ^2$.

(vii) C'est clair.

Remarque : L'hexagone de Pascal : on considère le triplet de droites

$$L_1:PAF\qquad L_2:QDE,\qquad L_3:RBC$$

et

$$M_1:PCD,\qquad M_2:QAB,\qquad M_3:REF$$

Soit $C_1=L_1+L_2+L_3$ et $C_2=M_1+M_2+M_3$. On a $C_1\cap C_2=\{A,B,C,D,E,F,P,Q,R\}$. Si PQR son colinéaires avec $L=PQR$; alors soit Γ la conique qui passe par $ABCDE$, par construction $L+\Gamma$ est un cubique qui passe

par les 8 points $\{A, B, C, D, E, P, Q, R\}$. D'après (5) (iv), il continet aussi F. Par hypothèse $F \notin L$ de sorte que $F \in \Gamma$, ce qui prouve que les six points appartiennent à une même conique.

Réciproquement, supposons que $ABCDEF$ sont sur une même conique Γ et soit $L = PQ$. Alors $L + \Gamma$ est un cubique qui passe par $\{A, B, C, D, E, F, P, Q, R\}$ et passe donc par R. Or R ne peut pas être sur Γ, sinon Γ serait dégénérée et les 6 droites ne seraient pas toutes distinctes. Ainsi $R \in L$ et PQR sont colinéaires.

4 1) Le discriminant de E est $64a^3$ et celui de F est $-432a^2$. Ils sont non nuls car on a $p \geq 5$. Par suite, E et F sont deux courbes elliptiques sur $\mathbb{F}_p$. 2) Soit N_p le nombre cherché. Pour tout $z \in \mathbb{F}_p$, notons $\chi(z) = \left(\frac{z}{p}\right)$ le symbole de Legendre (sur $\mathbb{F}_p$). Rappelons que l'on a

$$\chi(z) = \begin{cases} 0 & \text{si } z = 0 \\ 1 & \text{si } z \text{ est un carré non nul dans } \mathbb{F}_p \\ -1 & \text{sinon.} \end{cases}$$

Pour tout $u \in \mathbb{F}_p$, le nombre de solutions de l'équation $y^2 = u$ est $1 + \chi(u)$. Compte tenu du point à l'infini, on a donc

$$N_p = 1 + \sum_{x \in \mathbb{F}_p} \big(1 + \chi(x^3 - ax)\big) = p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 - ax). \tag{1}$$

Pour tout $x \in \mathbb{F}_p$, on a l'égalité

$$\chi\big((-x)^3 - a(-x)\big) = \chi(-1)\chi(x^3 - ax).$$

Puisque l'on a $p \equiv 3 \mod 4$, on a $\chi(-1) = -1$. Pour tout $x \in \mathbb{F}_p$, on a donc

$$\chi\big((-x)^3 - a(-x)\big) = -\chi(x^3 - ax).$$

Il résulte alors de (1) que l'on a $N_p = p + 1$. 3) Considérons l'application $f : \mathbb{F}_p^* \to \mathbb{F}_p^*$ qui à x associe x^3. C'est un morphisme de groupes. Il est injectif car on a $p \equiv 2 \mod 3$ (si $\mathbb{F}_p^*$ avait un élément d'ordre 3, $p - 1$ serait divisible par 3). Par suite, f est une bijection, i.e. tous les éléments de $\mathbb{F}_p^*$ sont des cubes. On en déduit que l'on a

$$\mathbb{F}_p = \Big\{x^3 - a \mid x \in \mathbb{F}_p\Big\}.$$

Si N_p est le nombre cherché, on a donc les égalités

$$N_p = 1 + \sum_{x \in \mathbb{F}_p} \big(1 + \chi(x^3 - a)\big) = p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x).$$

Puisqu'il y a exactement $\frac{p-1}{2}$ carrés non nuls dans $\mathbb{F}_p$, la somme des $\chi(x)$, pour x parcourant $\mathbb{F}_p$, est nulle, d'où $N_p = p + 1$.

5 1) Par définition de la loi de groupe sur E, les abscisses des points d'ordre 2 de $E(\mathbb{F}_{31})$ sont les racines dans $\mathbb{F}_{31}$ du polynôme $X^3 - 3X$. On a

$$\left(\frac{3}{31}\right) = -\left(\frac{31}{3}\right) = -1,$$

donc 3 n'est pas un carré dans $\mathbb{F}_{31}$. Le point $(0, 0)$ est donc le seul point d'ordre 2 de $E(\mathbb{F}_{31})$. Le sous-groupe cherché est donc $\big\{O, (0, 0)\big\}$, où O est le point à l'infini de E. 2) D'après l'exercice 1, l'ordre de $E(\mathbb{F}_{31})$ est 32. Afin de montrer que ce groupe est cyclique, prouvons le lemme suivant : *Lemme* Soit G un groupe abélien fini. Alors, G est cyclique si et seulement si pour tout nombre premier ℓ, G ne contient pas de sous-groupe isomorphe à $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.

Démonstration : la condition est évidemment nécessaire vu que tout sous-groupe d'un groupe cyclique est cyclique. Inversement, supposons que G ne contienne pas de sous-groupe isomorphe à $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. On écrit G comme somme directe de ses composantes ℓ-primaires :

$$G = \bigoplus_{\ell \,\big|\, |G|} G(\ell),$$

où $G(\ell)$ est la partie ℓ-primaire de G (i.e. l'ensemble des éléments de G annulés par une puissance de ℓ). Soit ℓ un diviseur premier de l'ordre de G. Compte tenu du théorème chinois, il suffit de vérifier que $G(\ell)$ est isomorphe $\mathbb{Z}/\ell^n\mathbb{Z}$ pour un certain entier $n \geq 1$. Si ce n'est pas le cas, il existe deux entiers n_1 et n_2 non nuls tels que $G(\ell)$

contienne un sous-groupe isomorphe à $\mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$. Ce dernier groupe contenant un sous-groupe isomorphe à $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, cela contredit l'hypothèse faite. D'où le lemme.

Supposons qu'il existe un nombre premier ℓ tel que $E(\mathbb{F}_{31})$ contienne un sous-groupe isomorphe à $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. Nécessairement, on a $\ell = 2$, et d'après la question 1 cela conduit à une contradiction, d'où l'assertion. Par ailleurs, le point $P = (3, 7) \in E(\mathbb{F}_{31})$ est un générateur. En effet, on a

$$2P = (2, 8), \quad 4P = (10, 3), \quad 8P = (20, 29), \quad 16P = (0, 0),$$

ce qui prouve que P est d'ordre 32.

Indiquons un autre argument pour vérifier que P est un générateur. On peut utiliser la question 4 de l'exercice 11 du premier envoi, en montrant que P n'est pas un double dans $E(\mathbb{F}_{31})$ i.e. qu'il n'existe pas $Q \in E(\mathbb{F}_{31})$ tel que $2Q = P$. S'il existait un tel point Q, d'après la formule de duplication sur E, il devrait exister $x \in \mathbb{F}_{31}$ tel que $x^4 + 19x^3 + 6x^2 + 5x + 9 = 0$, et l'on vérifie que ce n'est pas le cas.

6 1) Le discriminant de E vaut 1, donc E est une courbe elliptique sur $\mathbb{F}_2$. 2) Par définition de la loi de groupe sur E, on vérifie directement que l'on a

$$-P = (x, y + 1) \quad \text{et} \quad 2P = (x^4, y^4 + 1).$$

3) Soit $P = (x, y)$ un point de $E(\mathbb{F}_{16})$. Compte tenu de la question 2, on a

$$4P = 2(2P) = \big(x^{16}, (y^4 + 1)^4 + 1\big) = \big(x^{16}, y^{16}\big).$$

Puisque x et y sont dans $\mathbb{F}_{16}$, on a $x^{16} = x$ et $y^{16} = y$, d'où $4P = P$ et $3P$ est nul. Ainsi le point P, qui n'est pas le point à l'infini de E, est d'ordre 3. 4) Soit $P = (x, y)$ un point de $E(\mathbb{F}_{16})$. On a $2P = -P$, donc $x = x^4$ et $y = y^4$, ce qui entraîne que x et y sont dans $\mathbb{F}_4$ (les éléments de $\mathbb{F}_4$ sont exactement les racines du polynômes $X^4 - X$), d'où l'assertion. 5) D'après le théorème de Hasse, on a les inégalités

$$1 + 4 - 2\sqrt{4} \leq |E(\mathbb{F}_4)| \leq 1 + 4 + 2\sqrt{4} \quad \text{i.e.} \quad 1 \leq |E(\mathbb{F}_4)| \leq 9.$$

De même, on a

$$1 + 16 - 2\sqrt{16} \leq |E(\mathbb{F}_{16})| \leq 1 + 16 + 2\sqrt{16} \quad \text{i.e.} \quad 9 \leq |E(\mathbb{F}_{16})| \leq 25.$$

D'après la question précédente, on en déduit que $|E(\mathbb{F}_4)| = 9$.

7 Donnons tout d'abord le cardinal N de ce groupe noté G :

$$N = q + 1 + \sum_{x \in \mathbb{F}_{71}} \chi(x^3 - x)$$

où χ est le caractère donné par le symbole de Legendre. Comme $\chi\Big((-x)^3 - (-x)\Big) = \chi(-1)\chi(x^3 - x) = -\chi(x^3 - x)$ car $71 \equiv 3 \mod 4$ et donc $N = q+1 = 72$. Les points d'ordre 2 correspondent aux racines de $x^3 - x = x(x-1)(x+1)$ soit trois points. Comme G est de la forme $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$ avec $n|n'$ on en déduit que $n > 1$ avec le 2-Sylow de la forme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Il reste alors à déterminer les points d'ordre 3 soit $2P = -P$ ce qui revient à chercher les points P tels que P et $2P$ ont la même abscisse x soit :

$$(\frac{3x^2 - 1}{2y})^2 - 2x = x, \qquad (3x^2 - 1)^2 = 12xy^2 = 12x^4 - 12x^2$$

ce qui donne $3x^4 - 6x^2 - 1 = 0$. Or si x est une solution de cette équation alors $-x$ aussi mais alors$x^3 - x = -((-x)^3 - (-x))$ ne sont pas tous deux des carrés de sorte que l'on a au plus 4 solutions et donc en fait 2 et $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$.

8 D'après le théorème de structure des groupes abéliens finis, il existe au plus un couple d'entiers naturels non nuls (d_1, d_2) tel que $E(K)$ soit isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ et que d_1 divise d_2. Il suffit donc de démontrer l'assertion d'existence de l'énoncé. Pour tout diviseur premier p de l'ordre de $E(K)$, notons $E(p)$ la composante p-primaire de $E(K)$ i.e. l'ensemble de ses éléments d'ordre une puissance de p. Le groupe $E(K)$ est somme directe des $E(p)$. Par ailleurs, il existe des entiers naturels non nuls $n_1, \cdots, n_t$ tels que $n_i \leq n_{i+1}$ pour $i = 1, \cdots, t-1$ et que $E(p)$ soit isomorphe au groupe produit $\mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_t}\mathbb{Z}$. Puisque $\mathbb{Z}/p^{n_i}\mathbb{Z}$ contient un sous-groupe isomorphe à

$\mathbb{Z}/p\mathbb{Z}$ et que le sous-groupe de $E(K)$ formé des points annulés par p est d'ordre au plus p^2, on a $t \leq 2$. Autrement dit, il existe deux entiers r et s tels que l'on ait

$$E(p) \simeq \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z} \quad \text{avec} \quad s \geq 1 \quad \text{et} \quad 0 \leq r \leq s.$$

Le théorème chinois entraîne alors l'existence d'un couple d'entiers naturels (d_1, d_2) tel que

$$E(K) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \quad \text{avec} \quad d_1 \big| d_2.$$

Il reste à démontrer que d_1 divise $q-1$. On remarque pour cela que $\mathbb{Z}/d_2\mathbb{Z}$ contient un sous-groupe isomorphe à $\mathbb{Z}/d_1\mathbb{Z}$ (car d_1 divise d_2). Par suite, $E(K)$ contient un sous-groupe isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_1\mathbb{Z}$. Soit ℓ la caractéristique de K. L'entier d_1 n'est pas divisible par ℓ, sinon $E(K)$ contiendrait un sous-groupe isomorphe à $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, ce qui n'est pas. Si $\overline{K}$ est une clôture algébrique de K, le sous-groupe de $E\big(\overline{K}\big)$ formé des points annulés par d_1 est donc contenu dans $E(K)$. Il en résulte que le sous-groupe des racines d_1-ièmes de l'unité de $\overline{K}^*$ est contenu dans K, i.e. est un sous-groupe de K^*. Il est d'ordre d_1, donc d_1 divise $q-1$.

9 1) Soit r un entier ≥ 2. L'ensemble $E(\mathbb{F}_p)$ est un sous-groupe de $E(\mathbb{F}_{p^r})$. Montrons que c'est un sous-groupe propre de $E(\mathbb{F}_{p^r})$ i.e. que l'on a $E(\mathbb{F}_p) \neq E(\mathbb{F}_{p^r})$. D'après le théorème de Hasse, on a les inégalités

$$N_1 \leq p+1+2\sqrt{p} \quad \text{et} \quad p^r+1-2\sqrt{p^r} \leq N_r.$$

Vérifions l'inégalité

$$p+1+2\sqrt{p} < p^r+1-2\sqrt{p^r} \quad \text{i.e.} \ \big(\sqrt{p}+1\big)^2 < \big(\sqrt{p^r}-1\big)^2.$$

Il s'agit de prouver que l'on a $\sqrt{p}+1 < \sqrt{p^r}-1$. On remarque pour cela que $p \leq \sqrt{p^r}$ et p étant au moins 5, on a $\sqrt{p}+2 < p$. Puisque l'on a $r \geq 2$, cela entraîne $N_1 < N_r$, d'où notre assertion. D'après le théorème de Lagrange N_1 est donc un diviseur strict de N_r. Par ailleurs, d'après le théorème de Hasse, on a $p+1-2\sqrt{p} \leq N_1$. En utilisant l'inégalité $p \geq 5$, on en déduit que $N_1 \neq 1$, d'où le résultat. 2.1) On vérifie directement que $E(\mathbb{F}_2)$ est trivial i.e. est réduit au point à l'infini. La trace du Frobenius de E est donc $a = 2$. Par ailleurs, dans $\mathbb{Z}[T]$ on a (avec $i^2 = -1$)

$$2T^2 - 2T + 1 = (1-\alpha T)(1-\beta T) \quad \text{où} \quad \alpha = 1+i, \quad \beta = 1-i.$$

Compte tenu de la formule (1) de l'énoncé, on en déduit que l'on a par exemple

$$N_2 = 5, \quad N_3 = 13, \quad N_5 = 41, \quad N_7 = 113 \quad \text{et} \quad N_{11} = 2113.$$

2.2) On a l'égalité

$$N_r = 2^r + 1 - \Big((1+i)^r + (1-i)^r\Big). \tag{1}$$

Par ailleurs, on a

$$(1+i)^r = 2^{\frac{r}{2}} \exp\Big(\frac{r\pi i}{4}\Big) \quad \text{et} \quad (1-i)^r = 2^{\frac{r}{2}} \exp\Big(-\frac{r\pi i}{4}\Big).$$

Il en résulte que l'on a

$$(1+i)^r + (1-i)^r = 2^{\frac{r}{2}+1} \cos\Big(\frac{r\pi}{4}\Big). \tag{2}$$

Les égalités

$$\cos\Big(\frac{r\pi}{4}\Big) = \begin{cases} \frac{\sqrt{2}}{2} & \text{si } r \equiv \pm 1 \mod 8 \\ -\frac{\sqrt{2}}{2} & \text{si } r \equiv \pm 3 \mod 8 \end{cases} \quad \text{et} \quad \Big(\frac{2}{r}\Big) = (-1)^{\frac{r^2-1}{8}}, \tag{3}$$

entraînent alors le résultat. 2.3) L'équivalence des conditions 1 et 2 résulte directement de la question 2.2. Par ailleurs, d'après l'égalité (1) ci-dessus, on a

$$\Big|(1+i)^r - 1\Big|^2 = N_r. \tag{4}$$

Il en résulte que si N_r est premier, $(1+i)^r - 1$ satisfait à la condition (ii) de la question 8 de l'exercice 6 du premier envoi, il est donc irréductible. Inversement, supposons $x = (1+i)^r - 1$ irréductible dans $\mathbb{Z}[i]$. Compte tenu de (4) et de l'indication de l'énoncé, il suffit de montrer que x n'est pas associé à un nombre premier. Vérifions que x n'est pas dans $\mathbb{Z}$. Supposons le contraire. On alors $x = \overline{x}$, ce qui conduit à $(1+i)^{2r} = 2^r$ i.e. $i^r = 1$. Par hypothèse,

r est impair. En posant $r = 2k+1$, on obtient $i^{2k}i = 1$ i.e. $(-1)^k i = 1$, d'où une contradiction. Tout revient alors à vérifier que x n'est pas dans $i\mathbb{Z}$. Dans le cas contraire, on a $x + \overline{x} = 0$, autrement dit

$$(1+i)^r + (1-i)^r = 2.$$

D'après (2) et (3), on en déduit l'égalité

$$1 = 2^{\frac{r}{2}} \frac{\sqrt{2}}{2},$$

ce qui entraîne $r = 1$, puis $x = i$ et une contradiction. Cela établit l'équivalence des conditions 1 et 3 du lemme.

Il reste à vérifier que si l'une des conditions du lemme est satisfaite, alors r est premier. Soit d un diviseur de r. Puisque $\mathbb{F}_{2^d}$ est contenu dans $\mathbb{F}_{2^r}$, l'ensemble $E(\mathbb{F}_{2^d})$ est un sous-groupe de $E(\mathbb{F}_{2^r})$. Il en résulte que N_d divise N_r. Puisque N_r est premier, on a donc $N_d = 1$ ou $N_d = N_r$. Si $N_d = 1$, on a l'égalité $2^d = 2^{\frac{d+1}{2}}$ i.e. $d = 1$. Supposons $N_d = N_r$. On a alors

$$2^d - \Big(\frac{2}{d}\Big) 2^{\frac{d+1}{2}} = 2^r - \Big(\frac{2}{r}\Big) 2^{\frac{r+1}{2}}.$$

Les entiers d et r sont distincts de 1 car $N_1 = 1$ n'est pas premier. En exprimant le fait que les exposants de 2 dans la décomposition en facteurs premiers des deux membres de l'égalité ci-dessus sont égaux, on en déduit que l'on a $\frac{d+1}{2} = \frac{r+1}{2}$ i.e. $d = r$, d'où l'assertion. 2.4) D'après les égalités (1) et (2), qui ne dépendent pas de la parité de r, on a

$$N_r = 2^r + 1 - 2^{\frac{r}{2}+1} \cos\Big(\frac{r\pi}{4}\Big),$$

ce qui implique le résultat. Par ailleurs, pour tout entier r, si $2^r + 1$ est premier, alors r est une puissance de 2, et l'on a $N_2 = 5$. Cela entraîne la dernière assertion.

10 1) Notons N_r l'ordre du groupe $E(\mathbb{F}_{4^r})$. On vérifie que l'on a $N_1 = 1$. La trace du Frobenius de E est donc 4. Par ailleurs, on a $1 - 4T + 4T^2 = (1-2T)^2 \in \mathbb{Z}[T]$. D'après la formule (1) de l'énoncé de l'exercice 6, on a donc $N_r = 4^r + 1 - 2^{r+1} = (2^r - 1)^2$. 2) Soit $P = (x, y)$ un point de E. En utilisant la formule d'addition sur E, on vérifie directement que l'on a $2P = (x^4, y^4)$. 3) Soit $P = (x, y)$ un point de $E\big(\mathbb{F}_{4^r}\big)$. On déduit de la question 2 que l'on a l'égalité

$$2^r P = \big(x^{4^r}, y^{4^r}\big).$$

Puisque x et y appartiennent à $\mathbb{F}_{4^r}$, on a $x^{4^r} = x$ et $y^{4^r} = y$, d'où $2^r P = P$ et l'assertion. Par ailleurs, le groupe des points de E annulés par $2^r - 1$ est isomorphe au groupe produit $\mathbb{Z}/(2^r-1)\mathbb{Z} \times \mathbb{Z}/(2^r-1)\mathbb{Z}$. Compte tenu de la question 1, cela entraîne le résultat.