CHAPITRE 4

COURBES ELLIPTIQUES

4.1. Théorie générale

Ces premiers paragraphes sont un survol de (quelques) aspect algébrico-géométriques indissociables de la théorie des courbes elliptiques. Nous n'utiliserons (presque) jamais les termes ***variété*** ou ***schéma***, essayant de garder un point de vue le plus intuitif possible, au prix de quelques incorrections. Malgré l'utilisation de termes tels que ***ouvert*** ou ***fermé***, nous n'entrerons jamais dans des considérations topologiques. Il ne faut cependant pas oublier que la plupart des théorèmes que nous admettrons sont la conséquence de résultats géométriques profonds.

Dans tout ce qui suit, K désigne un corps, duquel on a fixé une clôture algébrique $\bar{K}$. En parlant d'extension (algébrique) de K, nous entendrons toujours un sous-corps de $\bar{K}$ contenant K. Par exemple, si K est fini, de cardinal q, alors, pour tout entier n, il existe un unique sous-corps de $\bar{K}$ de cardinal q^n (c'est le sous-ensemble de $\bar{K}$ formé par les racines du polynôme $X^{q^n} - X$, cf. le chapitre 6), que l'on notera comme d'habitude $\mathbb{F}_{q^n}$.

4.1.1. Espaces affines et projectifs — Voulant parler de courbes elliptiques, on ne peut se passer de définir la notion de plan projectif (ou, plus généralement, d'espace projectif) sur un corps. En effet, cet objet géométrique est l'« espace ambiant » dans lequelle elles sont construites.

On commence par définir la notion d'espace affine : pour tout entier n et tout anneau R, on pose $\mathbb{A}^n(R) = R^n$. Si R est un sous-anneau de S, on a une inclusion canonique $\mathbb{A}^n(R) \subset \mathbb{A}^n(S)$. L'ensemble $\mathbb{A}^n(\bar{K}) = \bar{K}^n$, noté $\mathbb{A}^n_K$, est appelé ***espace affine de dimension*** n ***sur*** K. En d'autre termes, un élément de $\mathbb{A}^n_K$ est un n-plet $P = (x_1, \ldots, x_n)$, avec $x_1, \ldots, x_n \in \bar{K}$. Pour toute extension L de K (contenue dans $\bar{K}$), on obtient une inclusion $\mathbb{A}^n(L) \subset \mathbb{A}^n_K$. Un élément de $\mathbb{A}^n(L)$ est appelé ***point*** L***-rationnel*** de $\mathbb{A}^n_K$ (ou simplement un ***point***, lorsque $L = \bar{K}$).

Exemple 4.1.1 —

1. L'espace $\mathbb{A}^1_K = \bar{K}$ est appelé ***droite affine*** (sur K).
2. L'espace $\mathbb{A}^2_K = \bar{K} \times \bar{K}$ est le ***plan affine*** (sur K).
3. Si K est fini, de cardinal q, alors $\mathbb{A}^n_K$ est inifini, mais $\mathbb{A}^n(K)$ est fini, de cardinal q^n.

On passe maintenant aux espaces projectifs : l'ensemble $\mathbb{A}^{n+1}(K) = K^{n+1}$ possède une structure canonique de K-espace vectoriel. On définit une relation d'équivalence sur $\mathbb{A}^{n+1}(K) - \{0\}$ en posant $u \sim v$ si et seulement s'il existe $\lambda \in K^\times$ tel que $v = \lambda u$. Le quotient de $\mathbb{A}^{n+1}(K) - \{0\}$ par cette relation est alors noté $\mathbb{P}^n(K)$. On remarquera que $\mathbb{P}^n(K)$ s'identitfie avec l'ensemble des droites vectorielles de K^{n+1} (i.e. les sous-espaces vectoriels de K^{n+1} de dimension 1). Si $P \in \mathbb{P}^n(K)$ est représenté par un vecteur $v \in K^{n+1}$, on écrira $P = [v]$.

Exercice 4.1.2 — Montrer que si L/K est une extension de corps alors on a une injection canonique $\mathbb{P}^n(K) \subset \mathbb{P}^n(L)$.

L'ensemble $\mathbb{P}^n_K = \mathbb{P}^n(\bar{K})$ est appelé ***espace projectif de dimension*** n ***sur*** K. En s'appuyant sur l'exercice ci-dessus, pour toute extension L de K (contenue dans $\bar{K}$), on a une injection canonique $\mathbb{P}^n(L) \subset \mathbb{P}^n_K$. Comme dans le cas affine, un élément P de $\mathbb{P}^n(L)$ est appelé ***point L-rationnel***.

Exercice 4.1.3 — Soit K un corps fini de cardinal q. Montrer que $\mathbb{P}^n(K)$ est fini, de cardinal $\frac{q^{n+1}-1}{q-1}$.

Pour mieux comprendre la structure des espaces projectifs, considérons le sous-ensemble

$$U = \{[x_0, \ldots, x_n] \in \mathbb{P}^n_K \mid x_n \neq 0\},$$

appelé ***ouvert (affine) standard***. L'application $f : U \to \mathbb{A}^n_K$ définie par

$$f([x_0, \ldots, x_n]) = \left(\frac{x_0}{x_n}, \ldots, \frac{x_{n-1}}{x_n}\right).$$

est bijective, sa réciproque $g : U \to \mathbb{A}^n_K$ étant donnée par

$$g(x_1, \ldots, x_n) = [x_1, \ldots, x_n, 1].$$

En d'autres termes, un point $P \in U$ possède un unique représentant du type $(x_0, \ldots, x_{n-1}, 1)$ et s'identifie avec l'élément $f(P) = (x_0, \ldots, x_{n-1})$ de $\mathbb{A}^n_K$. Le complémentaire de U est formé par les points du type $P = [x_0, \ldots, x_{n-1}, 0]$ et s'identifie canoniquement avec $\mathbb{P}^{n-1}_K$. En d'autres termes, l'espace $\mathbb{P}^n_K$ peut être vu comme union d'un espace affine de dimension n et d'un espace projectif de dimension $n-1$.

Exemple 4.1.4 —

1. L'espace projectif $\mathbb{P}^0_K$ est réduit à un point. En effet, pour tout $P \in \mathbb{P}^0_K$, on a $P = [x] = [1]$, avec $x \in \bar{K}^\times$.

2. L'espace $\mathbb{P}^1_K$ est appelé ***droite projective (sur K)***. L'ouvert standard U s'identifie avec $\mathbb{A}^1_K$ et son complénentaire est un point. En d'autres termes, $\mathbb{P}^1_K$ est l'union de $\bar{K}$ et d'un point « à l'infini ».
3. Finalement, l'espace $\mathbb{P}^2_K$ est appelé ***plan projectif (sur K)***. L'ensemble
$$U = \{[x, y, z] \in \mathbb{P}^2_K \mid z \neq 0\},$$
s'identifie avec $\mathbb{A}^2_K$. Son complémentaire D, que l'on assimile à $\mathbb{P}^1_K$, est la droite « à l'infini ».

4.1.2. Courbes algébriques planes — La ***courbe affine plane (sur K)*** associée à un polynôme non constant $f \in K[X, Y]$ est l'ensemble
$$C = \{(x, y) \in \mathbb{A}^2_K \mid f(x, y) = 0\}.$$
Pour toute extension L de K, on peut considérer l'ensemble $C(L) = C \cap \mathbb{A}^2(L)$ des points L-rationnels de C. On a donc $P = (x, y) \in C(L)$ si et seulement si $x, y \in L$ et $f(x, y) = 0$.

Exemple 4.1.5 — Soit $d \in \mathbb{F}_q$ un non-résidu quadratique (en particulier, q est impair) et considérons la courbe C sur $\mathbb{F}_q$ associée au polynôme $f = X^2 - dY^2$. Sur $\bar{\mathbb{F}}_q$ (et déjà sur $\mathbb{F}_{q^2}$), on a l'identité
$$f = (X - aY)(X + aY),$$
avec $a \in \bar{\mathbb{F}}_q$ vérifiant la relation $a^2 = d$. En particulier, C est l'union des deux droites d'équations $X = aY$ et $X = -aY$, s'intersectant en l'origine. Le problème est que ces deux droites ne sont pas définies sur $\mathbb{F}_q$, ce qui explique le fait que $C(\mathbb{F}_q)$ est réduit au simple point $(0, 0)$. On peut par ailleurs facilement montrer que $C(\mathbb{F}_{q^n})$ est de cardinal 1 pour n impair et $2q^n - 1$ si n est pair.

Voulant obtenir une construction analogue dans le cas du plan projectif, on commence par remarquer que la valeur d'un polynôme $f \in K[X, Y, Z]$ en un point $P = [x, y, z] \in \mathbb{P}^2_K$ n'est pas bien définie, car elle dépend du représentant $(x, y, z) \in \bar{K}^3$ de P. Afin de remédier à cet inconvénient, supposons que f est non nul et ***homogène*** de degré d, c'est à dire que, pour tout $\lambda \in \bar{K}$, on a l'identité
$$f(\lambda X, \lambda Y, \lambda X) = \lambda^d f(X, Y, Z).$$
La valeur de f en P n'est toujours pas bien définie. Par contre, les deux relations $f(P) = 0$ et $f(P) \neq 0$ ont un sens, car si $f(x, y, z) = 0$ (par exemple) alors, pour tout $\lambda \in \bar{K}^\times$, on obtient les identités
$$f(\lambda x, \lambda y, \lambda z) = \lambda^d f(x, y, z) = 0.$$
L'ensemble
$$C = \{[x, y, z] \in \mathbb{P}^2_K \mid f(x, y, z) = 0\}$$

est alors appelé ***courbe projective plane de degré*** d ***(sur*** K***)*** associé à f. On utilisera la notation

$$C : f = 0$$

pour désignér la courbe C. En reprenant les notations du paragraphe précédent, l'intersection

$$C \cap U = \{[x, y, z] \in C \mid z \neq 0\}$$

sera appelée ***partie affine*** de C, le plus souvent notée C^{aff}. Elle s'identifie avec la courbe affine plane associée au polynôme $f(X, Y, 1)$. En général, l'intersection $C \cap D$ (où D désigne le complémentaire de U), qui n'est autre que $C \setminus C^{\text{aff}}$, est un ensemble fini (sauf si Z ne divise pas f) et ses éléments peuvent être facilement déterminés. Réciproquement, soit C_0 la courbe affine plane associée à un polynôme non constant $g \in K[X, Y]$ de degré d. En considérant le polynôme homogène de degré d

$$f = Z^d g\left(\frac{X}{Z}, \frac{Y}{Z}\right) \in K[X, Y, Z],$$

la courbe C_0 s'identifie avec la partie affine de la courbe $C \subset \mathbb{P}^2_K$ associée à f. On dit que C est la ***projectifiée*** de C_0.

Exemple 4.1.6 —

1. La partie affine de la courbe C associée au polynôme $X^n+Y^n-Z^n$ est l'ensemble des points $P = (x, y) \in \mathbb{A}^2_K$ vérifiant $x^n + y^n = 1$.
2. Soit $d \in \mathbb{F}_q$ un non-résidu quadratique et considérons la courbe projective plane $C \subset \mathbb{P}^2_K$ définie par l'équation

   $$X^2 - dY^2 = Z^2.$$

   Sa partie affine C^{aff} s'identifie avec la courbe plane affine définie par l'équation

   $$X^2 - dY^2 = 1.$$

   Elle possède les deux points « à l'infini » $[a, 1, 0]$ et $[-a, 1, 0]$, où l'élément $a \in \bar{\mathbb{F}}_q$ vérifie l'identité $a^2 = d$. On en déduit en particulier, pour tout entier naturel impair n, l'inclusion $C(\mathbb{F}_{q^n}) \subset C^{\text{aff}}$.

4.1.3. Courbes elliptiques, équations de Weierstrass — À partir de maintenant, on suppose que la caractéristique de K ne divise pas 6. Une ***courbe elliptique*** (définie) sur K est une courbe projective plane sur K définie par une équation du type

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3,$$

avec $a, b \in K$ tels que

$$\Delta = \Delta(E) = -16(4a^3 + 27b^2) \neq 0.$$

Une telle équation est appelée ***équation de Weierstrass***. L'élément $\Delta \in K^\times$ est le ***discriminant*** de la courbe elliptique. On écrira souvent $E = E_{a,b}$. On vérifie

facilement que $0_E = [0, 1, 0]$ est le seul point à l'infini de E. La partie affine E^{aff} est définie par l'équation

$$Y^2 = X^3 + aX + b.$$

Pour toute extension L de K, on a donc l'identité $E(L) = E^{\text{aff}}(L) \cup \{0_E\}$.

Remarque 4.1.7 — La condition $\Delta \neq 0$ est équivalente à la ***lissité*** de la courbe, une notion technique qui certifie que E possède de « bonnes » propriétés géométriques et permet d'appliquer de puissant résultats généraux de géométrie algébrique. Dans le cas présent, il apparaît que cette condition est équivalente à la séparabilité du polynôme $X^3 + aX + b$ (i.e. le fait qu'il possède trois racines distinctes dans $\bar{K}$).

L'application bijective $\sigma : E \to E$ définie par

$$\sigma([x, y, z]) = [x, -y, z]$$

est appelée ***involution canonique*** de la courbe elliptique. Pour tout point P de E, on a clairement la relation $\sigma^2(P) = P$. On remarquera que σ définit une involution de E^{aff}, définie par la relation

$$\sigma(x, y) = (x, -y).$$

Les 4 points fixes de σ sont 0_E et les points $P = (x, 0) \in E^{\text{aff}}$, où $x \in \bar{K}$ est une racine du polynôme $X^3 + aX + b$.

4.1.4. La loi de groupe — Soit E une courbe elliptique sur K, définie par une équation de Weierstrass affine

$$Y^2 = X^3 + aX + b.$$

Nous allons maintenant définir une loi de composition interne

$$(P, Q) \mapsto P + Q$$

sur E, appelée ***loi de composition des cordes-tangentes***. Bien que nous n'ayons pas défini la notion de droite dans le plan projectif, de tangente à une courbe ou d'intersection de courbes planes, nous allons commencer par une description géométrique de cette loi, qui est bien plus visuelle et intuitive : considérons deux points $P, Q \in E$ et, pour $P \neq Q$ (resp. $P = Q$), soit D la droite passant par P et Q (resp. la tangente à E en P). On peut montrer que la droite D intersecte E en un troisième point R (c'est un cas particulier du théorème de Bézout). On pose alors $P + Q = \sigma(R)$, où σ désigne l'involution canonique de E.

Sans rentrer dans les détails, donnons directement la transcription algébrique de la consctruction ci-dessus, qu'il faudra donc prendre (dans le contexte de ce cours) comme définition (rigoureuse) de la loi des cordes-tangentes :

1. Pour tout $P \in E$, on pose

$$P + 0_E = 0_E + P = P \quad \text{et} \quad P + \sigma(P) = \sigma(P) + P = 0_E.$$

2. Si $P = (x, y)$ et $Q = (x', y')$ appartiennent à E^{aff} et $Q \neq \sigma(P)$, considérons les éléments λ et ν de $\bar{K}$ définis par

$$\lambda = \frac{y - y'}{x - x'} \quad \text{et} \quad \nu = \frac{xy' - x'y}{x - x'}$$

pour $P \neq Q$, et

$$\lambda = \frac{3x^2 + a}{2y} \quad \text{et} \quad \nu = \frac{ax + 2b - x^3}{2y}$$

lorsque $P = Q$. Le point $P + Q$ est alors égal à $\sigma(R)$, où $R = (x'', y'')$ est l'élément de E^{aff} défini par les relations

$$x'' = \lambda^2 - x - x' \quad \text{et} \quad y'' = \lambda x'' + \nu.$$

Exercice 4.1.8 — Vérifier que le point R défini ci-dessus appartient à E^{aff}.

Théorème 4.1.9 — *La loi de composition des cordes-tangente définit une structure de groupe abélien sur E ayant 0_E comme élément neutre, l'opposé d'un point $P \in E$ étant égal à $\sigma(P)$.*

Démonstration — La loi de composition est clairement commutative. La vérification de l'associativité est bien plus délicate ; nous l'admettrons. Il est possible, bien qu'assez fastidieux, de la déduire de l'expression explicite ci-dessus (nous invitons néanmoins le lecteur à le faire). Par définition, l'élément neutre est égal à 0_E et l'opposé de $P \in E$ est donné par $\sigma(P)$. □

Exemple 4.1.10 — D'après ce dernier théorème, un point $P \in E$ est d'ordre divisant 2 si et seulement si $\sigma(P) = P$. En effet, la relation $2P = 0_E$ est équivalente à $P = -P$. On en déduit que $E[2]$ est d'ordre 4, isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. En particulier, si E est donnée par l'équation de Weierstrass

$$Y^2 = X^3 + aX + b,$$

le sous-groupe $E[2]$ de E est formé par les éléments $0_E, P_1 = (x_1, 0), P_2 = (x_2, 0)$ et $P_3 = (x_3, 0)$, où x_1, x_2 et x_3 sont les racines de $X^3 + aX + b$ (cf. la remarque 4.1.7).

Proposition 4.1.11 — *Soit E une courbe elliptique sur K. Pour toute extension L de K (contenue dans $\bar{K}$), $E(L)$ est un sous-groupe de E.*

Démonstration — Il suffit de vérifier que 0_E appartient à $E(L)$ et que, étant donnés $P, Q \in E(L)$, on a $-P \in E(L)$ et $P + Q \in E(L)$. Les deux premières propriétés sont immédiates, la dernière découle des expressions explicites de la loi de groupe. □

Exemple 4.1.12 —

1. Soit E la courbe elliptique sur $\mathbb{Q}$ d'équation

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

Le point $P = (-1, 1)$ appartient à $E(\mathbb{Q})$. On vérifie que l'on a

$$2P = (6, -15), 3P = (\frac{11}{49}, \frac{617}{343}), 4P = (\frac{1081}{900}, -\frac{65771}{27000})$$
$$5P = (\frac{179051}{80089}, \frac{91814227}{22665187}), 6P = (-\frac{6465234}{18653761}, -\frac{130201927155}{80565593759}), \ldots.$$

En fait, on peut montrer que P est un point d'ordre infini et qu'il engendre $E(\mathbb{Q})$. Ce n'est pas un résultat simple, il faut développer la théorie des courbes elliptiques sur $\mathbb{Q}$ pour l'établir.

2. Supposons K fini, de cardinal q (premier avec 6) et considérons une courbe elliptique E sur K. L'ensemble $\mathbb{P}^2(K)$ étant de cardinal $q^2 + q + 1$ (cf. l'exercice 4.1.3), on en déduit que le groupe $E(K)$ est fini (là où E est infini), ceci étant d'ailleurs valable pour $E(L)$, où L est une quelconque extension finie de K. Un des objectifs principaux de la théorie des courbes elliptiques sur les corps finis consiste à déterminer l'ordre ainsi que la structure des groupes $E(L)$.

4.1.5. Interlude : groupes abéliens finis — Afin de continuer l'étude des courbes elliptiques, et en particulier de leurs points d'ordre fini, nous avons besoin de quelques résultats complémentaires en théorie des groupes. Soit G un groupe abélien. Un ***supplémentaire*** d'un sous-groupe H de G est un sous-groupe K de G tel que $G = HK$ (i.e. G est engendré par H et K) et $H \cap K = 1$.

Exercice 4.1.13 — Montrer que si K est un supplémentaire de H alors G est isomorphe au produit direct $H \times K$.

Lemme 4.1.14 — *Soit G un groupe abélien fini d'exposant n. Fixons un sous-groupe H de G d'exposant n. Tout homomorphisme $H \to \mathbb{Z}/n\mathbb{Z}$ s'étent en un homomorphisme $G \to \mathbb{Z}/n\mathbb{Z}$.*

Démonstration — Il suffit de montrer le résultat lorsque G est engendré par H et un unique élément $g \in G$. Notons K le sous-groupe de G engendré par g. Dans ce cas, le groupe $K' = H \cap K$ est engendré par g^m, avec $m = |K|/|K'|$. Considérons un homomorphisme de groupes $f : H \to \mathbb{Z}/n\mathbb{Z}$. Par hypothèse, on a $g^m \in H$ et l'élément $f(g^m)$ est d'ordre d divisant $|K'|$. Il existe alors un (unique) élément $r \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $f(g^m) = \frac{n}{d}r$. L'entier d divisant $|K'|$ et l'ordre de K divisant n, on en déduit que n/d est un multiple de m. On vérifie alors sans difficulté qu'en posant $f(g) = \frac{n}{md}r$, on étend f à G. □

Lemme 4.1.15 — *Soient G un groupe abélien fini et $H \subset G$ un sous-groupe cyclique. Si l'ordre de H coïncide avec l'exposant de G alors H possède un supplémentaire.*

Démonstration — Notons n l'exposant de G. Ayant fixé u générateur de H, on obtient un isomorphisme de groupes $f : H \to \mathbb{Z}/n\mathbb{Z}$. D'après le lemme précédent, f s'étend en un homomorphisme $f : G \to \mathbb{Z}/n\mathbb{Z}$, d'où un homomorphisme $\pi : G \to H$ tel que

$f(h) = h$ pour tout $h \in H$. En posant $K = \ker(H)$, on en déduit alors les relations $HK = G$ et $H \cap K = 1$, ce qui implique que K est un supplémentaire de H. □

Nous pouvons à présent montrer le ***théorème de structure des groupes abéliens finis***.

Théorème 4.1.16 — *Soit G un groupe abélien fini. Il existe alors des entiers $n_1, \ldots, n_k$, avec n_i divisant n_{i+1}, tels que G soit isomorphe au produit direct $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$.*

Démonstration — On procède par récurrence sur l'ordre n du groupe G. Pour $n = 1$, l'assertion est immédiate. Supposons donc $n > 1$ et la propriété démontrée pour tout groupe d'ordre strictement inférieur à n. D'après le lemme 3.3.6, le groupe G possède un sous-groupe cyclique H d'ordre m égal à son exposant et le lemme 4.1.15 affirme alors que H possède un supplémentaire K d'où des isomorphismes de groupes $G \cong K \times H \cong K \times \mathbb{Z}/m\mathbb{Z}$ (cf. l'exercice 4.1.13). Par hypothèse de récurrence, on a un isomorphisme $K \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$, avec $n_i | n_{i+1}$. On remarquera que dans ce cas, l'entier n_r est l'exposant de K et divise donc m (car l'exposant d'un sous-groupe divise l'exposant du groupe), d'où le résultat. □

4.1.6. Structure de la torsion — L'étude des points de torsion est un aspect incontournable de la théorie des courbes elliptiques. Pour tout entier n, notons $E[n]$ le sous-groupe de E formé par les points P tels que $nP = 0_E$, i.e. le noyau de l'endomorphisme de multiplication par n. Le résultat suivant sera admis. Sa démonstration nécessite une étude approfondie des courbes elliptiques, qui ne serait envisageable dans ce cours.

Théorème 4.1.17 — *Soient E une courbe elliptique sur un corps K de caractéristique p et ℓ un nombre premier.*

1. *L'endomorphisme $E \to E$ de mutliplication par ℓ est surjectif.*
2. *Si ℓ est différent de la caractéristique de K alors le groupe $E[\ell]$ est fini, d'ordre ℓ^2.*
3. *Si $\ell = p$, on a deux possibilités :*
   (a) *Le groupe $E[p]$ est fini, d'ordre p, auquel cas on dit que E est **ordinaire**.*
   (b) *Le groupe $E[p]$ est trivial, et E est dite **supersingulière**.*

Le premier point du théorème affirme que tout point P de E est ***ℓ-divisible***, i.e. qu'il existe un point $Q \in E$ tel que $P = \ell Q$. On en déduit facilement que E est n-divisible pour tout entier $n > 0$. Les deux points suivants sont cruciaux car ils affirment que $E[\ell]$ est fini, en exhibant son ordre. En utilisant le théorème de structure des groupes abéliens finis, démontré dans le chapitre 5, on peut déduire de ce dernier résultat la structure des groupes $E[n]$ pour tout entier n.

Théorème 4.1.18 — *Soient E une courbe elliptique définie sur un corps K et $n > 0$ un entier.*

1. *Si K est de caractéristique 0, le groupe $E[n]$ est isomorphe au produit $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*
2. *Si K est de caractéristique $p > 0$, posons $n = mp^r$ avec m premier à p. On a un isomorphisme*

$$E[n] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \text{si } E \text{ est ordinaire,} \\ \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \text{si } E \text{ est supersingulière.} \end{cases}$$

Démonstration — Considérons la factorisation $n = \prod_\ell \ell^{e_\ell}$. Le groupe $E[n]$ est alors isomorphe au produit $\prod_\ell E[\ell^{e_\ell}]$. Il suffit donc de déterminer la structure de $E[n]$ dans le cas $n = \ell^e$. Supposons d'abord $\ell \neq p$. Montrons, par récurrence sur l'entier $e > 0$, que $E[\ell^e]$ est d'ordre ℓ^{2e}. Pour $e = 1$, on retrouve le point 2 du théorème 4.1.17. Soit donc $e > 0$ un entier et supposons $E[\ell^e]$ d'ordre ℓ^{2e}. Le groupe $E[\ell^{e+1}]$ coïncide avec la préimage de $E[\ell^e]$ par l'endomorphisme de multiplication par ℓ. Le point 1 et le point 2 du théorème 4.1.17 impliquent alors que $E[\ell^{e+1}]$ est d'ordre $\ell^2|E[\ell^e]| = \ell^{2(e+1)}$, d'où l'assertion.

D'après le théorème 4.1.16, le groupe $E[\ell^e]$ est isomorphe à un produit

$$\mathbb{Z}/\ell^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/\ell^{e_r}\mathbb{Z},$$

avec $0 < e_1 \leq e_2 \leq \cdots \leq e_r$, l'entier ℓ^{e_r} étant l'exposant de $E[\ell^e]$. En particulier, on a l'identité $e_1 + \cdots + e_r = 2e$ et l'inégalité $e_r \leq e$. Si l'on avait $r > 2$, le groupe $E[\ell^{e_1}] \subset E[\ell^e]$ serait d'ordre $\ell^{re_1} > \ell^{2e_1}$, ce qui est exclu. Pour $r = 1$, le groupe $E[\ell^e]$ serait cyclique, d'ordre ℓ^{2e}, ce qui est impossible, car son exposant divise ℓ^e. On a donc $r = 2$ et $E[\ell^e]$ est isomorphe à $\mathbb{Z}/\ell^{e_1}\mathbb{Z} \times \mathbb{Z}/\ell^{e_2}\mathbb{Z}$, avec $0 < e_1 \leq e_2 \leq e$ et $e_1 + e_2 = 2e$. On vérifie facilement que la seule possibilité est donnée par $e_1 = e_2 = e$. Le sous-groupe $E[\ell^e]$ est donc isomorphe au produit $\mathbb{Z}/\ell^e\mathbb{Z} \times \mathbb{Z}/\ell^e\mathbb{Z}$.

Pour $\ell = p$, si $E[p]$ n'est pas trivial, on procède comme précédemment, en montrant d'abord que $E[p^e]$ est d'ordre p^e (en s'appuyant sur le théorème 4.1.17), puis qu'il est cyclique (en appliquant le théorème de structure des groupes abéliens finis). Finalement, si $E[p]$ est trivial, il en est de même pour $E[p^e]$, pour tout entier $e \geq 1$. □

4.1.7. Équivalence — Ayant fixé le corps K, nous venons de construire une famille de groupes $E_{a,b}(L)$, dépendant de deux paramètres a et b de K ainsi que d'une extension L de K (contenue dans $\bar{K}$). Il est naturel de se demander comment ces groupes varient en fonction de a, b et L. Dans ce paragraphe, nous allons partiellement répondre à cette question en définissant la notion d'équivalence entre courbes elliptiques. Nous verrons en effet que des choix particuliers de a et b amènent à des courbes elliptiques qui peuvent être naturellement identifiées.

Soient $E = E_{a,b}$ et $E' = E_{a',b'}$ deux courbes elliptique sur K et fixons une extension quelconque L de K (pas nécessairement contenue dans $\bar{K}$). Nous dirons que E et E' sont ***L-équivalentes*** s'il existe un élément $\lambda \in L^\times$ tel que

$$\begin{cases} a' = \lambda^4 a, \\ b' = \lambda^6 b. \end{cases}$$

Nous utiliserons les notations $E \sim_L E'$ et $E' = \lambda \cdot E$. Remarquons que l'on a alors l'identité

$$\Delta(E') = \lambda^{12}\Delta(E).$$

On en déduit en particulier que λ est racine du polynôme

$$X^{12} - \frac{\Delta(E')}{\Delta(E)} \in K[X]$$

et est donc algébrique sur K. Voulant étudier la notion de L-équivalence, on peut donc se réduire au cas habituel où le corps L est contenu dans $\bar{K}$.

Pour une valeur arbitraire de $\lambda \in \bar{K}^\times$, la courbe elliptique $E' = \lambda \cdot E$ n'est généralement pas définie sur K. Nous dirons que λ est ***admissible*** pour E si E' est définie sur K, i.e. si $\lambda^4 a$ et $\lambda^6 b$ sont des éléments de K. Tel est le cas par exemple si $\lambda^2 \in K$: pour tout $t \in K^\times$, ayant fixé une racine carré $\sqrt{t}$ de t dans $\bar{K}$, la courbe elliptique $E' = \sqrt{t} \cdot E$ sur K est définie par l'équation

$$Y^2 = X^3 + t^2 aX + t^3 b.$$

On remarquera que E' ne dépend pas du choix de la racine carrée de t. Si t est un carré de K alors E et E' sont K-équivalentes. Si t n'est pas un carré, on dira que E' est une ***tordue (quadratique)*** de E (par rapport à $\sqrt{t}$).

Remarque 4.1.19 — Malgré le fait que t ne soit pas un carré de K, il est possible que E et sa tordue quadratique $\sqrt{t} \cdot E$ soient K-équivalentes (ou même qu'elle coïncident). On vérifie facilement que ce phénomène se produit si et seulement si $E = E_{a,0}$ et $-t$ est un carré de K.

Exercice 4.1.20 — Soit $E = E_{a,b}$ une courbe elliptique sur K. Montrer que $\lambda \in \bar{K}$ est admissible pour E si et seulement si $\lambda^{2m} \in K^\times$, où $m = 3$ si $a = 0$, $m = 2$ pour $b = 0$ et $m = 1$ sinon.

L'intérêt de la notion de $\bar{K}$-équivalence repose sur le fait que si $E' = \lambda \cdot E$, avec λ admissible pour E, alors non seulement les groupes E et E' sont isomorphes, mais il en est également de même pour $E(L)$ et $E'(L)$, pour toute extension L de $K(\lambda)$. Afin de rendre cette affirmation plus précise, pour tout $\lambda \in \bar{K}^\times$, considérons l'application $f_\lambda : \mathbb{P}^2_K \to \mathbb{P}^2_K$ définie par

$$f_\lambda([x, y, z]) = [\lambda^2 x, \lambda^3 y, z].$$

Proposition 4.1.21 — *Soient E une courbe elliptique sur K, $\lambda \in \bar{K}^\times$ un élément admissible pour E et posons $E' = \lambda \cdot E$. Pour toute extension L de $K(\lambda)$, l'application f_λ définit un isomorphisme de groupes de $E(L)$ sur $E'(L)$.*

Démonstration — Vérifions d'abord que, pour tout $P \in E(L)$, on a $f_\lambda(P) \in E'(L)$. On a clairement $f_\lambda(0_E) = 0_E = 0_{E'}$. Soit donc $P = (x, y) \in E^{\mathrm{aff}}(L)$, de telle sorte que $f(P) = (\lambda^2 x, \lambda^3 y) \in \mathbb{A}^2(L)$ (car x, y et λ appartiennent à L). On a alors les identités

$$y'^2 = \lambda^6 y^2 = \lambda^6(x^3 + ax + b) = \lambda^6 x^3 + \lambda^6 ax + \lambda^6 b = x'^3 + \lambda^4 ax' + \lambda^6 b$$

et le point $f_\lambda(P)$ appartient à $E'(L)$. L'application f_λ est bijective, sa réciproque étant donnée par $g(x, y) = (\lambda^{-2}x, \lambda^{-3}y)$. Le fait que f_λ soit un homomorphisme de groupe est une simple vérification : soit $Q = (x', y') \in E(L)$ un second point L-rationnel. Nous ne traiterons que le cas $Q \neq \pm P$, auquel cas on a l'identité $P + Q = (x'', y'')$, avec

$$x'' = \left(\frac{y - y'}{x - x'}\right)^2 - x - x'.$$

De même, on obtient $f_\lambda(P) + f_\lambda(Q) = (x''', y''')$, avec

$$x''' = \left(\frac{\lambda^3 y - \lambda^3 y'}{\lambda^2 x - \lambda^2 x'}\right)^2 - \lambda^2 x - \lambda^2 x' = \lambda^2 x''.$$

De manière analogue, on obtient l'identité $y''' = \lambda^3 y''$. On a donc la relation $f_\lambda(P + Q) = f_\lambda(P) + f_\lambda(Q)$. □

Exemple 4.1.22 — Considérons une courbe elliptique $E = E_{a,b}$ sur $\mathbb{F}_q$ et posons $E' = \sqrt{-1} \cdot E$. Distinguons deux cas :

1. Pour $b \neq 0$, la caractéristique de K étant différente de 2, on a les relations $E' = E_{a,-b} \neq E'$. Si q est congru à 1 modulo 4, i.e. si -1 est un carré dans $\mathbb{F}_q$, alors E et E' sont $\mathbb{F}_q$-équivalentes et, pour tout entier $n > 0$, les groupes $E(\mathbb{F}_{q^n})$ et $E'(\mathbb{F}_{q^n})$ sont isomorphes. Si q est congru à 3 modulo 4, alors E et E' sont seulement $\mathbb{F}_{q^2}$-équivalentes et, en général, seuls les groupes $E(\mathbb{F}_{q^{2n}})$ et $E'(\mathbb{F}_{q^{2n}})$ sont isomorphes. Par exemple, pour $q = 7$ et $E = E_{1,1}$, le groupe $E(\mathbb{F}_7)$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$, mais $E'(\mathbb{F}_7)$ est isomorphe à $\mathbb{Z}/11\mathbb{Z}$. Par contre, $E(\mathbb{F}_{49})$ et $E'(\mathbb{F}_{49})$ sont tous deux isomorphes ŝ $\mathbb{Z}/55\mathbb{Z}$.
2. Pour $b = 0$, on a l'identité $E' = E$. Fixons $\lambda \in \bar{K}$ avec $\lambda^2 = -1$. D'après la proposition 4.1.21, l'application f_λ définit un automorphisme de $E = E(\bar{K})$ et on a $f_\lambda(E(K)) = E(K)$ si et seulement si -1 est un carré dans K.

Afin d'étudier la notion de $\bar{K}$-équivalence, on associe à une courbe elliptique $E = E_{a,b}$ son ***invariant modulaire***, qui est l'élément $j(E) \in K$ défini par

$$j(E) = -110592\frac{a^3}{\Delta(E)} \in K.$$

D'après les hypothèses faites sur K et suite à la factorisation $110592 = 2^{12} \cdot 3^3$, on a $j(E) = 0$ si et seulement si $a = 0$. La courbe E est alors définie par une équation du type

$$Y^2 = X^3 + b.$$

De même, l'identité

$$j(E) - 1728 = 746496 \frac{b^2}{\Delta(E)},$$

avec $746496 = 2^{10} \cdot 3^6$, implique que $j(E) = 1728$ si et seulement si $b = 0$, ce qui correspond à une équation du type

$$Y^2 = X^3 + aX.$$

Nous verrons que les cas $j(E) = 0$ et $j(E) = 1728$ sont particuliers et devront systématiquement être traités séparément.

Théorème 4.1.23 — *Deux courbes elliptiques E et E' sur K sont $\bar{K}$-équivalentes si et seulement si on a l'identité $j(E) = j(E')$.*

Démonstration — Posons $E = E_{a,b}$ et $E' = E_{a',b'}$. On commence par remarquer que si $E' = \lambda \cdot E$, avec $\lambda \in \bar{K}$, alors on a les relations $a' = \lambda^6 a$ et $\Delta(E') = \lambda^{12}\Delta(E)$, d'où l'identité $j(E') = j(E)$. Réciproquement, si cette dernière condition est remplie, on distingue trois cas :

1. Si $a = 0$ (i.e. si $j(E) = 0$) alors $a' = 0$ et $bb' \neq 0$ (car $\Delta(E)\Delta(E') \neq 0$). Dans ce cas, on a l'identité $E' = \lambda \cdot E$, où $\lambda \in \bar{K}$ est une racine sixième de $b^{-1}b'$.
2. Si $b = 0$ (i.e. si $j(E) = 1728$) alors $b' = 0, aa' \neq 0$ et on a la relation $E' = \lambda \cdot E$, où λ est une racine quatrième de $a^{-1}a' \in \bar{K}^\times$.
3. Pour $ab \neq 0$ (auquel cas $a'b' \neq 0$), l'identité $j(E) = j(E')$ se traduit par la relation
$$a^3 b'^2 = a'^3 b^2.$$
On vérifie alors facilement l'identité $E' = \lambda \cdot E$, où $\lambda \in \bar{K}^\times$ est une racine carrée de l'élément
$$\mu = \frac{ab'}{a'b}.$$

□

Nous pouvons maintenant étudier plus en détail la notion de K-équivalence. Deux courbes elliptiques K-équivalentes ont le même invariant modulaire, mais la réciproque est fausse si K n'est pas algébriquement clos (il suffit par exemple de considérer la tordue quadratique d'une courbe elliptique, telle qu'elle a été définie précédemment). On introduit alors un second invariant, noté δ, qui, associé à l'invariant modulaire j, permet de décrire complètement les classes de K-équivalence. Étant donnée une courbe elliptique $E = E_{a,b}$ sur K, on distingue trois cas :

1. Si $j(E) = 0$ alors $\delta(E)$ est l'image de $b \in K^\times$ dans $K^\times/(K^\times)^6$.
2. Si $j(E) = 1728$ alors $\delta(E)$ est l'image de $a \in K^\times$ dans $K^\times/(K^\times)^4$.
3. Sinon, $\delta(E)$ est l'image de $a^{-1}b \in K$ dans $K^\times/(K^\times)^2$.

Corollaire 4.1.24 — *Deux courbes elliptiques E et E' sur K sont K-équivalentes si et seulement si $j(E) = j(E')$ et $\delta(E) = \delta(E')$.*

Démonstration — Posons $E = E_{a,b}$ et $E' = E_{a',b'}$. Si E et E' sont K-équivalentes alors elles sont $\bar{K}$-équivalentes et la proposition 4.1.23 affirme que l'on a l'identité $j(E) = j(E')$. Supposons que $j(E) \neq 0, 1728$. En posant $E' = \lambda \cdot E$, avec $\lambda \in K^\times$, on obtient les relations

$$\frac{b'}{a'} = \lambda^2 \frac{b}{a},$$

d'où l'identité $\delta(E) = \delta(E')$. Réciproquement, si $j(E) = j(E')$ et $\delta(E) = \delta(E')$, alors E et E' sont $\bar{K}$-équivalentes et nous avons vu dans la démonstration de la proposition 4.1.23 que $E' = \lambda \cdot E$, où $\lambda \in \bar{K}^\times$ est une racine carrée de $\frac{ab'}{a'b}$. L'identité $\delta(E) = \delta(E')$ implique alors que λ appartient à $K^\times$. Les courbes elliptiques E et E' sont donc K-équivalentes. Les cas $j(E) = 0$ et $j(E) = 1728$ se traitent de la même manière. □

Proposition 4.1.25 — *Soient $j \in K$ et $\delta \in K^\times/(K^\times)^{2m}$, avec $m = 3$ pour $j = 0$, $m = 2$ pour $j = 1728$ et $m = 1$ sinon. Il existe une courbe elliptique E sur K telle que $j(E) = j$ et $\delta(E) = \delta$.*

Démonstration — Soit $t \in K^\times$ un représentant de δ. Pour $j \neq 0, 1728$, en considérant la courbe elliptique

$$E = E_{at^2,at^3} = \sqrt{t} \cdot E_{a,a}$$

sur K, avec

$$a = -\frac{27j}{4(j - 1728)},$$

on vérifie facilement les relations $\Delta(E) \neq 0, j(E) = j$ et $\delta(E) = \delta$. Pour $j = 0$ (resp. $j = 1728$), il suffit de considérer la courbe elliptique $E_{0,t}$ (resp. $E_{t,0}$). □

En combinant le corollaire 4.1.24 et la proposition 4.1.25, on en déduit qu'il existe une bijection entre les classes de K-équivalences de courbes elliptiques sur K et l'ensemble des couples (j, δ), avec $j \in K$ et $\delta \in K^\times/(K^\times)^{2m}$, où m est défini comme ci-dessus.

Remarque 4.1.26 — Étant données deux courbes elliptiques E et E' sur K, il est clairement possible que les groupes $E(K)$ et $E'(K)$ soient isomorphes sans que E et E' soient K-équivalentes. Si K est un corps fini, ceci peut se produire, par exemple, lorsque E et E' sont ***isogènes*** (nous n'aborderons pas cette notion).

Exemple 4.1.27 — Déterminons le nombre de classes de $\mathbb{F}_q$-équivalence de courbes elliptiques sur $\mathbb{F}_q$: tout d'abord, il existe q classes de $\bar{\mathbb{F}}_q$-équivalence, correspondant aux valeurs possibles de l'invariant modulaire $j \in \mathbb{F}_q$. Afin de décrire les classes de $\mathbb{F}_q$-équivalence, distinguons plusieurs cas :

- Pour $j \neq 0, 1728$, le groupe $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$ étant d'ordre 2, chaque classe de $\bar{\mathbb{F}}_q$-équivalence se décompose en deux classes de $\mathbb{F}_q$-équivalence. Si une courbe elliptique appartient à l'une de ces classes alors une quelconque de ses tordues quadratiques appartient à l'autre classe.
- Supposons maintenant $j = 0$. Si q est congru à 1 modulo 6, le groupe $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^6$ est d'ordre 6 et on obtient donc 6 classes de $\mathbb{F}_q$-équivalence. Si q est congru à -1 modulo 6, le groupe $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^6$ est isomorphe à $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$ et on n'a que deux classes de $\mathbb{F}_q$-équivalence.
- Posons finalement $j = 1728$. Pour q congru à 1 modulo 4, le groupe $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^4$ est d'ordre 4 et on obtient 4 classes de $\mathbb{F}_q$-équivalence. Pour q congru à 3 modulo 4, les groupes $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^4$ et $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$ sont isomorphes et on obtient deux classes de $\mathbb{F}_q$-équivalence.

En résumant, le nombre de classes de $\mathbb{F}_q$-équivalence de courbes elliptiques sur $\mathbb{F}_q$ est égal à

$$2(q + e_0 + e_{1728}),$$

avec

$$e_0 = \begin{cases} 2 \text{ si } q \equiv 1 \pmod 6, \\ 0 \text{ si } q \equiv 5 \pmod 6 \end{cases} \quad \text{et} \quad e_{1728} = \begin{cases} 1 \text{ si } q \equiv 1 \pmod 4, \\ 0 \text{ si } q \equiv 3 \pmod 4. \end{cases}$$

Remarquons que pour $j \neq 0, 1728$, chaque classe de $\mathbb{F}_q$-équivalence est formée de $\frac{1}{2}(q-1)$ courbes elliptiques (de type $E_{a,b}$) sur $\mathbb{F}_q$.

4.2. Courbes elliptiques sur les corps fini

Nous avons déjà obtenu des résultats concernant les courbes elliptiques sur les corps finis (en énumérant, par exemple, le nombre de classes de K-équivalence de courbes elliptiques sur $\mathbb{F}_q$), ceux-ci se plaçant dans un contexte théorique général. Dans cette section nous aborderons des aspects qui sont propres aux corps finis, tels que l'endomorphisme de Frobenius ou des techniques de comptage de points par le symbole de Legendre.

4.2.1. Complexité — Voulant utilliser les courbes elliptiques pour des applications cryptographiques, il es naturel d'étudier la complexité de la loi de groupe.

Proposition 4.2.1 — *Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$. La loi de groupe sur $E(\mathbb{F}_q)$ est de complexité $O(\log^3(q))$.*

Démonstration — Soit E une courbe elliptique sur $\mathbb{F}_q$ et considérons deux points $P, Q \in E(\mathbb{F}_q)$. En reprenant la définition de la loi de groupe sur E, la partie la plus « coûteuse » pour calculer $P+Q$ est constituée par les divisions dans le calcul de λ et ν. Nous avons vu que la complexité d'une division dans $\mathbb{F}_q$ (ou de la détermination d'un inverse) est de complexité $O(\log^3(q))$. Toutes les autres opérations intervenant dans le calcul de $P+Q$ étant de complexité au plus $O(\log^2(q))$ (leur nombre ne dépendant pas de q), on en déduit le résultat. □

La taille d'un point de $E(\mathbb{F}_q)$ est clairement mesurée par la taille de ses coordonnées, qui, étant des éléments de $\mathbb{F}_q$, sont de l'ordre de $\log(q)$ (cf. le chapitre 6), On en déduit que les courbes elliptiques sur les corps finis se prêtent à des applications cryptographiques, la structure de groupe étant de complexité polynomiale par rapport à la taille de ses éléments.

4.2.2. La borne de Hasse — Étant donnée une courbe elliptique E définie sur $\mathbb{F}_q$, le groupe $E(\mathbb{F}_q)$ est fini, car il est contenu dans $\mathbb{P}^2(\mathbb{F}_q)$, qui est de cardinal p^2+p+1. Afin de déterminer son ordre, on peut utiliser une généralisation du symbole de Legendre (cf. le chapitre 2) : étant donné $x \in \mathbb{F}_q$, on pose

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} 0 \text{ si } x = 0, \\ 1 \text{ si } x \in \mathbb{F}_q^\times \text{ est un carré}, \\ -1 \text{ sinon.} \end{cases}$$

Exercice 4.2.2 — En reprenant les techniques utilisées dans le chapitre 2, montrer que dans $\mathbb{F}_q$, on a l'identité

$$\left(\frac{x}{\mathbb{F}_q}\right) = x^{\frac{q-1}{2}}.$$

En déduire qu'étant donnés $x, y \in \mathbb{F}_q$, on a la relation

$$\left(\frac{xy}{\mathbb{F}_q}\right) = \left(\frac{x}{\mathbb{F}_q}\right)\left(\frac{y}{\mathbb{F}_q}\right).$$

Proposition 4.2.3 — *Soit E une courbe elliptique sur $\mathbb{F}_q$, définie par une équation affine*

$$Y^2 = X^3 + aX + b.$$

On a l'identité

$$|E(\mathbb{F}_q)| = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3+ax+b}{\mathbb{F}_q}\right).$$

Démonstration — Le point 0_E étant toujours défini sur $\mathbb{F}_q$, il suffit de déterminer le cardinal de $E^{\text{aff}}(\mathbb{F}_q)$. Un élément $P = (x, y) \in E^{\text{aff}}$ appartient à $E^{\text{aff}}(\mathbb{F}_q)$ si et seulement si $x \in \mathbb{F}_q$ et $x^2 + ax + b$ est un carré dans $\mathbb{F}_q$. En particulier, étant donné $x \in K$, si $x^3 + ax + b$ n'est pas un carré alors x ne se réalise pas comme abscisse d'un point de $E^{\text{aff}}(\mathbb{F}_q)$. Pour $x^3 + ax + b = 0$, on obtient un unique point $P = (x, 0) \in$

$E^{\mathrm{aff}}(\mathbb{F}_q)$. Finalement, si $x^3+ax+b=y^2$ est un carré non nul de $\mathbb{F}_q$ alors on obtient les points $P=(x,y)$ et $-P=(x,-y)$. Pour tout $x\in\mathbb{F}_q$, on a les relations

$$1+\left(\frac{x^3+ax+b}{\mathbb{F}_q}\right)=\begin{cases}0 \text{ si } x^3+ax+b \text{ n'est pas un carré dans } \mathbb{F}_q,\\ 1 \text{ si } x^3+ax+b=0,\\ 2 \text{ sinon.}\end{cases}$$

On en déduit les identités

$$\begin{aligned}|E(\mathbb{F}_q)| &= 1+|E^{\mathrm{aff}}(\mathbb{F}_q)| = 1+\sum_{x\in\mathbb{F}_q}\left(1+\left(\frac{x^3+ax+b}{\mathbb{F}_q}\right)\right)=\\ &= q+1+\sum_{x\in\mathbb{F}_q}\left(\frac{x^3+ax+b}{\mathbb{F}_q}\right).\end{aligned}$$

□

Dans la section 4.1.7, nous avons vu que si deux courbes elliptiques E et E' sur $\mathbb{F}_q$ sont $\mathbb{F}_q$-équivalentes alors les groupes $E(\mathbb{F}_q)$ et $E'(\mathbb{F}_q)$ sont isomorphes, donc de même ordre. Dans cette même section, nous avons défini la tordue quadratique $\sqrt{t}\cdot E$, où $t\in\mathbb{F}_q^\times$ n'est pas un carré.

Corollaire 4.2.4 — *Soient E et E' deux courbes elliptiques sur $\mathbb{F}_q$. Si E' est une tordue quadratique de E alors on a l'identité*

$$|E(\mathbb{F}_q)|+|E'(\mathbb{F}_q)|=2q+2.$$

Démonstration — Posons $E=E_{a,b}$ et $E'=\sqrt{t}\cdot E=E_{t^2a,t^3b}$ où $t\in K^\times$ n'est pas un carré. L'application $x\mapsto tx$ étant une bijection de $\mathbb{F}_q$, on en déduit les relations

$$\begin{aligned}|E'(\mathbb{F}_q)| &= q+1+\sum_{x\in\mathbb{F}_q}\left(\frac{x^3+t^2ax+t^3b}{\mathbb{F}_q}\right)=\\ &= q+1+\sum_{x\in\mathbb{F}_q}\left(\frac{(tx)^3+t^2a(tx)+t^3b}{\mathbb{F}_q}\right)=\\ &= q+1+\sum_{x\in\mathbb{F}_q}\left(\frac{t}{\mathbb{F}_q}\right)\left(\frac{x^3+ax+b}{\mathbb{F}_q}\right)=\\ &= q+1-\sum_{x\in\mathbb{F}_q}\left(\frac{x^3+ax+b}{\mathbb{F}_q}\right)=2q+2-|E(\mathbb{F}_q)|.\end{aligned}$$

□

Corollaire 4.2.5 — *Soit E une courbe elliptique sur $\mathbb{F}_q$, avec q congru à 3 modulo 4. Si $j(E)=1728$ alors $E(\mathbb{F}_q)$ est d'ordre $q+1$.*

Démonstration — D'après la définition d'invariant modulaire, on a $j(E) = 1728$ si et seulement si $E = E_{a,0}$, avec $a \in K^\times$. Pour $q \equiv 3 \pmod 4$, l'élément $-1 \in K$ n'est pas un carré et $\sqrt{-1} \cdot E = E$ est donc une tordue quadratique de E (cf. la remarque 4.1.19). Le corollaire précédent permet de conclure. □

Remarque 4.2.6 — L'exemple 4.1.27 affirme que pour $q \equiv 3 \pmod 4$, il existe exactement deux classes de $\mathbb{F}_q$ équivalence de courbes elliptiques sur $\mathbb{F}_q$ d'invariant modulaire 1728, représentées respectivement par $E = E_{1,0}$ et $E' = E_{-1,0}$. D'après le corollaire 4.2.5, les groupes $E(\mathbb{F}_q)$ et $E'(\mathbb{F}_q)$ sont tous deux d'ordre $q+1$. Ils ne sont cependant pas isomorphes. En effet, $E(\mathbb{F}_q)$ possède un unique point d'ordre 2 et $E'(\mathbb{F}_q)$ en possède trois. Nous verrons plus loin qu'il est possible de décrire complètement la structure de ces deux groupes.

Le résultat suivant, connu sous le nome de ***borne de Hasse*** est fondamental. Sa démonstration nécessitant des techniques qu'il serait impossible d'introduire dans ce cours, nous n'en donnerons que l'énoncé.

***Théorème 4.2.7* (Hasse)** — *Soit E une courbe elliptique sur $\mathbb{F}_q$. On a l'inégalité*

$$|q + 1 - |E(\mathbb{F}_q)|| \leq 2\sqrt{q}.$$

L'intervalle

$$H_q = [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}] = \left[(\sqrt{q} - 1)^2, (\sqrt{q} + 1)^2\right]$$

est appelé ***intervalle de Hasse***. Le résultat ci-dessus peut être reformulé en disant que $|E(\mathbb{F}_q)|$ appartient à H_q. Il est possible de montrer que si q est un nombre premier, tout entier de H_q apparaît comme ordre du groupe des points $\mathbb{F}_q$-rationnels d'une courbe elliptique définie sur $\mathbb{F}_q$ (ce résultat étant faux en général).

Corollaire 4.2.8 — *Si E est une courbe elliptique sur $\mathbb{F}_q$ alors le groupe $E(\mathbb{F}_q)$ est non trivial.*

Démonstration — D'après les hypothèses faites sur $\mathbb{F}_q$, on a $q \geq 5$, ce qui entraîne les relations

$$|E(\mathbb{F}_q)| \geq (\sqrt{q} - 1)^2 \geq (\sqrt{5} - 1)^2 > 1.$$

□

Exercice 4.2.9 — Soient x et y deux réels positifs. Montrer que l'on a l'inégalité $|x + 1 - y| \leq 2\sqrt{x}$ si et seulement si $|y + 1 - x| \leq 2\sqrt{y}$. En déduire que pour toute courbe elliptique E sur $\mathbb{F}_q$, on a la relation

$$||E(\mathbb{F}_q)| + 1 - q| \leq 2\sqrt{|E(\mathbb{F}_q)|}.$$

4.2.3. L'endomorphisme de Frobenius — Pour tout entier $n > 0$, l'application $\mathrm{Fr}_q : \mathbb{A}^n_{\mathbb{F}_q} \to \mathbb{A}^n_{\mathbb{F}_q}$ définie par

$$\mathrm{Fr}_q(x_1, \ldots, x_n) = (x_1^q, \ldots, x_n^q)$$

est appelée ***morphisme de Frobenius***. On a la relation $\mathrm{Fr}_q(P) = P$ si et seulement si $P \in \mathbb{A}^n(\mathbb{F}_q)$, généralisant ainsi la relation $x^q = x$ si et seulement si $x \in \mathbb{F}_q$ (qui correspond au cas $n = 1$). Soient $P = (x_0, \ldots, x_n)$ et $Q = (y_0, \ldots, y_n)$ deux points de $\mathbb{A}^{n+1}_{\mathbb{F}_q}$. S'il existe $\lambda \in \overline{\mathbb{F}}_q$ tel que $y_i = \lambda x_i$ pour tout $i \in \{0, \ldots, n\}$ alors on obtient les identités $y_i^q = \lambda^q x_i^q$. On en déduit que le morphisme de Frobenius définit une application $\mathrm{Fr}_q : \mathbb{P}^n_{\mathbb{F}_q} \to \mathbb{P}^n_{\mathbb{F}_q}$.

Exercice 4.2.10 — Montrer que l'application $\mathrm{Fr}_q : \mathbb{P}^n_{\mathbb{F}_q} \to \mathbb{P}^n_{\mathbb{F}_q}$ est bijective et que, pour tout point $P \in \mathbb{P}^n_{\mathbb{F}_q}$, on a $\mathrm{Fr}_q(P) = P$ si et seulement si $P \in \mathbb{P}^n(\mathbb{F}_q)$.

Soit E une courbe elliptique sur $\mathbb{F}_q$, définie par une équation de Weierstrass affine

$$Y^2 = X^3 + aX + b.$$

On a l'identité $\mathrm{Fr}_q(0_E) = 0_E$ et, étant donné $P = (x, y) \in E^{\mathrm{aff}}$, on a les relations

$$(y^q)^2 = (y^2)^q = (x^3 + ax + b)^q = x^{3q} + a^q x^q + b^q = (x^q)^3 + ax^q + b,$$

d'où $\mathrm{Fr}_q(P) \in E^{\mathrm{aff}}$ (les éléments a et b appartenant à $\mathbb{F}_q$, ils sont fixés par Fr_q). On en déduit que le morphisme de Frobenius induit une bijection $E \to E$.

Remarque 4.2.11 — Étant donnée une courbe projective plane C, on obtient une bijection $\mathrm{Fr}_q : C \to C$ telle que, pour tout $P \in C$, on a $\mathrm{Fr}_q(P) = P$ si et seulement si $P \in C(\mathbb{F}_q)$ et, plus généralement, pour tout entier $n > 0$, on a $\mathrm{Fr}_q^n(P) = P$ si et seulement si $P \in C(\mathbb{F}_{q^n})$.

Proposition 4.2.12 — *L'application* $\mathrm{Fr}_q : E \to E$ *est un endomorphisme de groupe.*

Démonstration — Considérons deux éléments P et Q de E. Nous devons montrer que $\mathrm{Fr}_q(P + Q) = \mathrm{Fr}_q(P) + \mathrm{Fr}_q(Q)$. Cette relation étant évidente pour $P = 0_E$ ou $Q = 0_E$, nous pouvons supposer que $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ appartiennent à E^{aff}. Comme dans la démonstration du théorème 4.1.21, nous ne traiterons que le cas $Q \neq \pm P$, auquel cas on a l'identité $P + Q = (x_3, y_3)$, avec

$$x_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2.$$

De même, on obtient $\mathrm{Fr}_q(P) + \mathrm{Fr}_q(Q) = (x_4, y_4)$, avec

$$x_4 = \left(\frac{y_1^q - y_2^q}{x_1^q - x_2^q}\right)^2 - x_1^q - x_2^q = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^{2q} - (x_1 - x_2)^q = x_3^q.$$

De manière analogue, on obtient l'identité $y_4 = y_3^q$, d'où le résultat. □

On en déduit immédiatement le corollaire suivant, qui fournit une démonstration alternative du fait que $E(\mathbb{F}_{q^n})$ est un groupe.

Corollaire 4.2.13 — *Pour tout entier n, le sous-groupe $E(\mathbb{F}_{q^n})$ de E est le noyau de l'endomorphisme $1 - \mathrm{Fr}_q^n$.*

Le fait que le morphisme de Frobenius soit un endomorphisme (bijectif) de E implique, en particulier, qu'il induit un endomorphisme

$$E[n] \xrightarrow{\mathrm{Fr}_q} E[n]$$

pour tout entier naturel n. Nous avons vu que si $n = \ell$ est un nombre premier différent de la caractéristique p de $\mathbb{F}_q$, le groupe $E[\ell]$ est un $\mathbb{F}_\ell$-espace vectoriel de dimension 2. En particulier, Fr_q définit un élément du groupe $\mathrm{GL}(E[\ell])$. En d'autres termes, ayant fixé une $\mathbb{F}_\ell$-base de $E[\ell]$, l'endomorphisme Fr_q est représenté par une matrice A appartenant à $\mathrm{GL}_2(\mathbb{F}_\ell)$. On peut en particulier parler de la ***trace***

$$\mathrm{tr}_\ell(\mathrm{Fr}_q) = \mathrm{tr}(A) \in \mathbb{F}_\ell,$$

du ***déterminant***

$$\det_\ell(\mathrm{Fr}_q) = \det(A) \in \mathbb{F}_\ell^\times$$

et, plus généralement, du ***polynôme caractéristique***

$$\chi_\ell = X^2 - \mathrm{tr}_\ell(\mathrm{Fr}_q)X + \det_\ell(\mathrm{Fr}_q) \in \mathrm{Fr}_\ell[X]$$

de l'endomorphisme Frobenius agissant sur $E[\ell]$, ceux-ci étant indépendants de la $\mathbb{F}_\ell$-base considérée. Le théorème de Cayley-Hamilton affirme alors que dans $\mathrm{GL}(E[\ell])$ on a la relation

$$\chi_\ell(\mathrm{Fr}_q) = 0,$$

c'est à dire que, pour tout $P \in E[\ell]$, on a l'identité

$$\mathrm{Fr}_q^2(P) - \mathrm{tr}_\ell(\mathrm{Fr}_q)\,\mathrm{Fr}_q(P) + \det_\ell(\mathrm{Fr}_q)P = 0_E.$$

On remarquera également que $\mathrm{Fr}_q^2 = \mathrm{Fr}_q \circ \mathrm{Fr}_q = \mathrm{Fr}_{q^2}$.

Exemple 4.2.14 — Considérons la courbe elliptique E sur $\mathbb{F}_{11}$ définie par l'équation

$$Y^2 = X^3 + X + 3$$

Soit $\alpha \in \mathbb{F}_{121}$ une racine carrée de 2. On vérifie facilement que les points $P = (1, 4)$ et $Q = (2, \alpha)$ sont d'ordre 3. De plus, ils forment une $\mathbb{F}_3$-base de $E[3]$. En effet, s'ils étaient linéairement dépendants, il existerait un entier n tel que $Q = nP$, et Q appartiendrait donc à $E(\mathbb{F}_{11})$, ce qui est exclu. Les relations $\mathrm{Fr}_{11}(P) = P$ et $\mathrm{Fr}_{11}(Q) = -Q$ impliquent que la matrice associée à Fr_{11} dans la base (P, Q) est donnée par

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

On en déduit les identités $\mathrm{tr}_3(\mathrm{Fr}_{11}) = 0, \det_3(\mathrm{Fr}_{11}) = -1$ et $\chi_3 = X^2 - 1$.

Remarque 4.2.15 — De manière plus générale, pour tout entier naturel n premier à p, on obtient un endomorphisme bijectif

$$E[n] \xrightarrow{\mathrm{Fr}_q} E[n].$$

Le groupe $E[n]$ est un $\mathbb{Z}/n\mathbb{Z}$-module libre de rang 2 [(1)] et, une fois fixée une $\mathbb{Z}/n\mathbb{Z}$-base, on associe à Fr_q une matrice $A \in \mathrm{GL}_n(\mathbb{Z}/n\mathbb{Z})$ (groupe des matrices à coefficients dans $\mathbb{Z}/n\mathbb{Z}$, de déterminant inversible). On peut une fois de plus définir la trace $\mathrm{tr}_n(\mathrm{Fr}_q) = \mathrm{tr}(A) \in \mathbb{Z}/n\mathbb{Z}$, le déterminant $\det_n(\mathrm{Fr}_q) \in (\mathbb{Z}/n\mathbb{Z})^\times$, le polynôme caractéristique

$$\chi_n = X^2 - \mathrm{tr}_n(\mathrm{Fr}_q) + \det_n(\mathrm{Fr}_q) \in \mathbb{Z}/n\mathbb{Z}[X]$$

et, dans $\mathrm{GL}(E[n])$, on a une fois de plus la relation $\chi_n(\mathrm{Fr}_q) = 0$.

Le résultat ci-dessous est profond et, comme nous le verrons, ses applications sont nombreuses. Il n'est malheureusement pas possible d'en donner une démonstration dans le contexte de ce cours.

Théorème 4.2.16 — *Soit E une courbe elliptique définie sur $\mathbb{F}_q$ et posons*

$$\chi = X^2 - tX + q \in \mathbb{Z}[X],$$

avec $t = q + 1 - |E(\mathbb{F}_q)|$.

1. *Dans l'anneau d'endomorphismes de E, on a la relation $\chi(\mathrm{Fr}_q) = 0$, i.e. pour tout $P \in E$, on a l'identité*

$$\mathrm{Fr}_q^2(P) - t\,\mathrm{Fr}_q(P) + qP = 0_E.$$

2. *Pour tout entier natuel n premier à p, le polynôme χ_n est la réduction modulo n de χ. En d'autres termes, on a les congruences*

$$\begin{cases} \mathrm{tr}_n(\mathrm{Fr}_q) \equiv t \pmod{n}, \\ \det_n(\mathrm{Fr}_q) \equiv q \pmod{n}. \end{cases}$$

L'entier t du théorème 4.2.16 est appelé ***trace*** de l'endomorphisme de Frobenius et χ est son ***polynôme caractéristique***.

Exemple 4.2.17 — Reprenons la courbe elliptique E sur $\mathbb{F}_{11}$ de l'exemple précédent. Nous avons vu que $\mathrm{tr}_3(\mathrm{Fr}_{11}) = 0$ et $\det_3(\mathrm{Fr}_{11}) = -1$. Un calcul direct par la méthode du symbole de Legendre montre que $E(\mathbb{F}_{11})$ est d'ordre 18. On obtient alors $t = -6$, ce qui donne $\chi = X^2 + 6X + 11$. On a bien les congruences

$$-6 \equiv 0 \pmod{3} \quad \text{et} \quad 11 \equiv -1 \pmod{3}.$$

1. Nous n'avons pas défini (et ne le ferons pas) la notion de module libre (de type fini) sur un anneau. Il suffit de savoir qu'elle généralise la structure d'espace vectoriel sur un corps. La plupart des résultats classiques d'algèbre linéaire restent valables dans ce nouveau contexte (existence d'une base, théorème du rang, applications linéaires et matrices, déterminants, théorème de Cayley-Hamilton,...)

4.2.4. Structure du groupe des points rationnels — L'ordre du groupe des points $\mathbb{F}_q$-rationnels d'une courbe elliptique peut être calculé en utilisant la méthode du symbole de Legendre décrite précédemment (ou des techniques plus performantes, telles que l'algorithme de Schoof). Déterminer sa structure de groupe est bien plus délicat. Nous verrons à présent comment le théorème 4.2.16 permet de faciliter la tâche.

Théorème 4.2.18 — *Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Le groupe $E(\mathbb{F}_q)$ est isomorphe au produit $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, où m est l'exposant de $E(\mathbb{F}_q)$ et n est un entier divisant le pgcd de m et $q-1$.*

Démonstration — Le théorème de structure des groupes abéliens finis affirme que $E(\mathbb{F}_q)$ est isomorphe au produit direct $\mathbb{Z}/m\mathbb{Z} \times G$, où G est un groupe abélien d'ordre $n = \frac{|E(\mathbb{F}_q)|}{m}$ et d'exposant divisant m. Si G n'était pas cylcique, il possèderait un sous-groupe isomorphe à $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, où ℓ est un nombre premier. Le nombre premier ℓ divisant m, le groupe $E(\mathbb{F}_q)$ possèderait un sous-groupe isomorphe à $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. Ce dernier serait alors contenu dans $E[\ell]$, qui est d'ordre ℓ^2 (au plus), ce qui est exclu. Montrons maintenant que n divise $q-1$. Tout d'abord, l'entier n divisant m, le groupe $E(\mathbb{F}_q)$ possède un sous-groupe isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, qui est clairement contenu dans $E[n]$. En comparant les ordres, on en déduit que $E[n]$ est contenu dans $E(\mathbb{F}_q)$ et que n n'est pas divisible par la caractéristique p de $\mathbb{F}_q$. En particulier, l'endomorphisme de Frobenius opère trivialement sur $E[n]$, i.e. $\mathrm{Fr}_q(P) = P$ pour tout $P \in E[n]$. On en déduit l'identité $\det_n(\mathrm{Fr}_q) = 1$ dans $\mathbb{Z}/n\mathbb{Z}$. D'autre part, le théorème 4.2.16, affirme que l'on a la congruence

$$\det_n(\mathrm{Fr}_n) \equiv q \pmod{n},$$

d'où le résultat. □

Exemple 4.2.19 —

1. Supposons q congru à 3 modulo 4 et considérons une fois de plus les deux classes de $\mathbb{F}_q$-équivalence de courbes elliptiques sur $\mathbb{F}_q$ d'invariant modulaire égal à 1728, représentées par les courbes $E = E_{1,0}$ et $E' = E_{-1,0}$. Nous avons vu que les groupes $E(\mathbb{F}_q)$ et $E'(\mathbb{F}_q)$ sont tous deux d'ordre $q+1$. Déterminons à présent leur structure. Le théorème ci-dessus affirme que $E(\mathbb{F}_q)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, avec n divisant $(m, q-1)$. L'exposant d'un groupe divisant son ordre, on en déduit que n divise $(q+1, q-1) = 2$ (la caractéristique de $\mathbb{F}_q$ est toujours supposée strictement supérieure à 3). On a $n = 2$ si et seulement si $E[2]$ est contenu dans $E(\mathbb{F}_q)$. La courbe E étant définie par l'équation de Weierstrass
$$Y^2 = X^3 + X,$$
et -1 nétant pas un carré dans $\mathbb{F}_q$, le groupe $E(\mathbb{F}_q)$ ne possède qu'un élément d'ordre 2. On a donc $n = 1$ et $E(\mathbb{F}_q)$ est cyclique. En répétant la même procédure

avec la courbe E', qui est définie par l'équation

$$Y^2 = X^3 - X$$

on montre que $E'(\mathbb{F}_q)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/\frac{q+1}{2}\mathbb{Z}$.

2. En supposant q congru à -1 modulo 6, considérons maintenant la courbe elliptique E sur $\mathbb{F}_q$ définie par l'équation

$$Y^2 = X^3 - 1.$$

L'homomorphisme de groupe $f : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$ défini par $f(x) = x^3$ est injectif. En effet, son noyau est le sous-groupe $\mathbb{F}_q^\times[3]$, qui est trivial car 3 ne divise pas l'ordre de $\mathbb{F}_q^\times$. On en déduit que l'application $f : \mathbb{F}_q \to \mathbb{F}_q$ définie par $f(x) = x^3$ est elle aussi injective, donc surjective, sa réciproque étant donnée par $x \mapsto x^{\frac{2q-1}{3}}$. Il s'en suit que l'application $h : \mathbb{F}_q \to E^{\mathrm{aff}}(\mathbb{F}_q)$ définie par

$$h(y) = \left((y+1)^{\frac{2q-1}{3}}, y\right)$$

est bijective. En particulier, le groupe $E(\mathbb{F}_q)$ est d'ordre $q+1$. Comme précédemment, on montre que $E(\mathbb{F}_q)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, avec n divisant 2. Le polynôme $X^3 - 1 = (X-1)(X^2+X+1)$ est scindé sur $\mathbb{F}_q$ si et seulement si -3 est un carré dans $\mathbb{F}_q$. Posons $q = p^n$, avec p premier. Dans ce cas, p est congru à 2 modulo 3 et n est impair. On en déduit les relations

$$\left(\frac{-3}{\mathbb{F}_q}\right) = \left(\frac{N_{\mathbb{F}_q/\mathbb{F}_p}(-3)}{p}\right) = \left(\frac{(-3)^n}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = -1.$$

On a donc $n = 1$ et $E(\mathbb{F}_q)$ est cyclique d'ordre $q+1$.

3. Montrons qu'il n'existe pas de courbe elliptique E sur $\mathbb{F}_q$ telle que $E(\mathbb{F}_q)$ soit isomorphe à $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$. Supposons par l'absurde qu'une telle courbe existe. D'après le théorème 4.2.18, l'entier q est congru à 1 modulo 11. Par ailleurs, l'exercice 4.2.9 affirme que q appartient à l'intervalle $[100, 144]$. Les seules puissances de nombres premiers dans cet intervalle sont $101, 103, 107, 109, 113, 11^2, 5^3, 127, 2^7, 131, 137$ et 139 et aucun de ces entiers est congru à 1 modulo 11.

4.2.5. Cardinal dans une extension finie du corps de base — Soit E une courbe elliptique sur $\mathbb{F}_q$. En s'appuyant sur le théorème 4.2.16, nous allons maintenant montrer que si l'on connaît le cardinal de $E(\mathbb{F}_q)$, on peut facilement en déduire le cardinal de $E(\mathbb{F}_{q^n})$. Commençons par quelques résultats préliminaires : soit

$$\chi = X^2 - tX + q \in \mathbb{Z}[X]$$

le polynôme caractéristique de l'endomorphisme de Frobénius et notons α et β ses deux racines dans $\mathbb{C}$, de telle sorte que

$$\chi = (X - \alpha)(X - \beta),$$

$t = \alpha + \beta$ et $q = \alpha\beta$. Considérons la suite $(u_n)_{n\geq 0}$ définie par

$$u_n = \alpha^n + \beta^n.$$

Lemme 4.2.20 — *Pour tout entier $n \geq 0$, le nombre complexe u_n est un entier.*

Démonstration — On procède par récurrence sur n : l'affirmation est vraie pour $n = 0$ et $n = 1$, car $u_0 = 2$ et $u_1 = t$. Soit $n > 1$ et supposons que u_n soit un entier pour tout entier naturel $m < n$. On a alors les relations

$$tu_{n-1} = (\alpha+\beta)t_{n-1} = (\alpha+\beta)(\alpha^{n-1}+\beta^{n-1}) = \alpha^n + \beta^n + \alpha^{n-1}\beta + \beta^{n-1}\alpha = \\ = u_n + \alpha\beta(\alpha^{n-2}+\beta^{n-2}) = u_n + qu_{n-2},$$

d'où l'identité

$$u_n = tu_{n-1} - qu_{n-2},$$

ce qui montre que u_n est un entier et fournit, enre autre, une méthode récursive de calcul des termes de la suite (u_n). □

Lemme 4.2.21 — *Si $\psi = X^2 - uX + q \in \mathbb{Z}[X]$ un vérifie la relation $\psi(\mathrm{Fr}_q) = 0$, alors $u = t$.*

Démonstration — Si $\psi(\mathrm{Fr}_q) = \chi(\mathrm{Fr}_q) = 0$, on obtient les relations

$$\psi(\mathrm{Fr}_q) - \chi(\mathrm{Fr}_q) = (u-t)\,\mathrm{Fr} = 0,$$

Ce qui se traduit par

$$(u-t)\,\mathrm{Fr}_q(P) = \mathrm{Fr}_q((u-t)P) = 0_E,$$

pour tout $P \in E$. L'endomorphisme de Frobenius étant injectif, on en déduit que $(u-t)P = 0_E$ pour tout $P \in E$. Si l'on avait $u - t \neq 0$, le groupe E, qui est infini, serait contenu dans le groupe fini $E[u-t]$, ce qui est absurde. On a donc $u = t$. □

Nous pouvons maintenant énoncer et démontrer le résultat principal de ce paragraphe.

Théorème 4.2.22 — *Avec les hypothèses et notations ci-dessus, pour tout entier strictement positif n, on a l'identité*

$$|E(\mathbb{F}_{q^n})| = q^n + 1 - u_n.$$

Démonstration — Posons $t_n = q+1-E(\mathbb{F}_{q^n})$. Dans se cas, le théorème 4.2.16 affirme que le polynôme $X^2 - t_nX + q^n \in \mathbb{Z}[X]$ annule Fr_{q^n}. En posant $\psi_n = X^2 - u_nX + q^n$, on a les identités

$$\psi_n(X^n) = X^{2n} - u_nX^n + q^n = (X^n - \alpha^n)(X^n - \beta^n) = (X-\alpha)(X-\beta)h_n = \chi_1 h_n,$$

avec $h_n \in \mathbb{C}[X]$. On montre facilement que h_n appartient à $\mathbb{Z}[X]$. En tenant compte de l'identité $\mathrm{Fr}_{q^n} = \mathrm{Fr}_q^n$, on obtient les relations

$$\psi_n(\mathrm{Fr}_{q^n}) = \chi_1(\mathrm{Fr}_q)h_n(\mathrm{Fr}_q) = 0.$$

En remplaçant Fr_q par Fr_{q^n}, le lemme précédent affirme alors que $t_n = u_n$, d'où le résultat. □

Exemple 4.2.23 — Considérons la courbe elliptique $E = E_{1,0}$ sur $\mathbb{F}_5$ définie par l'équation

$$Y^2 = X^3 + X.$$

En utilisant la méthode du symbole de Legendre, on obtient les relations

$$|E(\mathbb{F}_5)| = 6 + \left(\frac{0}{5}\right) + \left(\frac{2}{5}\right) + \left(\frac{0}{5}\right) + \left(\frac{0}{5}\right) + \left(\frac{3}{5}\right) = 6 - 2 = 4.$$

Le polynôme $X^3 + X = X(X-2)(X+2)$ étant scindé sur $\mathbb{F}_5$, on en déduit que $E(\mathbb{F}_5) = E[2]$. Les racines du polynôme caractéristique $\chi = X^2 - 2X + 5$ sont $\alpha = 1+2i$ et $\beta = 1-2i$. En appliquant le théorème 4.2.22, on en déduit que $|E(\mathbb{F}_{25}|$ est d'ordre

$$25 + 1 - (1+2i)^2 - (1-2i)^2 = 32.$$

Le théorème 4.2.18 affirme que les candidats possibles pour $E(\mathbb{F}_{25})$ sont $\mathbb{Z}/32\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. En tenant compte du fait que $E[2]$ est contenu dans $E(\mathbb{F}_{25})$, la première possibilité est écartée. Il reste à déterminer si $E[4]$ est contenu dans $E(\mathbb{F}_{25})$. Remarquons que pour tout $P \in E[4]$, on a $2P \in E[2]$, d'où $\mathrm{Fr}_5(2P) = 2P$. En utilisant le théorème 4.2.16, on obtient alors les relations

$$\mathrm{Fr}_{25}(P) = \mathrm{Fr}_5^2(P) = 2\,\mathrm{Fr}_5(P) - 5P = \mathrm{Fr}_5(2P) - 5P = 2P - 5P = -3P = P,$$

ce qui implique que P appartient à $E(\mathbb{F}_{25})$. On en déduit que $E(\mathbb{F}_{25})$ est isomorphe au produit direct $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

4.2.6. Ordinarité et supersingularité — Nous avons vu qu'en caractéristique positive, la structure de la p-torsion (ou, plus généralement, de la p^n-torsion) dépend de la courbe elliptique, ce qui n'est pas le cas en caractéristique nulle. Ceci amène à une distinction entre courbes ordinaires (pour lesquelles la p-torsion est non triviale) et supersingulière (pour lesquelles la p-torsion est triviale). Nous allons à présent étudier cette question de manière plus détaillée dans le cas des corps finis.

Théorème 4.2.24 — *Soit E une courbe elliptique définie sur $\mathbb{F}_q$, avec $q = p^r$, et posons $t = q + 1 - |E(\mathbb{F}_q)|$. Les conditions suivantes sont équivalentes :*

1. *E est supersingulière.*
2. *t est divisible par p.*

Démonstration — D'après les théorèmes de Cauchy et Lagrange, la courbe E est supersingulière si et seulement si, pour tout entier n, l'ordre du groupe $E(\mathbb{F}_{q^n})$ n'est pas divisible par p. En posant $t_n = q^n + 1 - |E(\mathbb{F}_{q^n})|$, on a la congruence

$$|E(\mathbb{F}_{q^n})| \equiv 1 - t_n \pmod{p}.$$

Dans la démonstration du lemme 4.2.20, nous avons vu que les entiers t_n vérifient la relation

$$t_n = tt_{n-1} - qt_{n-2}.$$

On en déduit la congruence

$$t_n \equiv t^n \pmod{p},$$

d'où

$$|E(\mathbb{F}_{q^n})| \equiv 1 - t^n \pmod{p}.$$

En particulier, si t n'est pas divisible par p alors t^{p-1} est congru à 1 modulo p et donc $E(\mathbb{F}_{q^{p-1}})$ possède un élément d'ordre p. Réciproquement, si q est divisible par p alors, pour tout entier $n > 0$, le groupe $E(\mathbb{F}_{q^n})$ est d'ordre congru à 1 modulo p et ne peut donc pas posséder d'élément d'ordre p. □

Exercice 4.2.25 — Soit E une courbe elliptique ordinaire définie sur $\mathbb{F}_q$ et notons $\mathbb{F}_q(E[p])$ la plus petite extension K de $\mathbb{F}_q$ telle que $E[p]$ soit contenu dans $E(K)$. Montrer que $\mathbb{F}_q(E[p]) = \mathbb{F}_{q^n}$, où n est l'ordre de $1 - |E(\mathbb{F}_q)|$ dans $\mathbb{F}_p^\times$.

Corollaire 4.2.26 — *Soit $p > 3$ un nombre premier. Une courbe elliptique E sur $\mathbb{F}_p$ est supersingulière si et seulement si $E(\mathbb{F}_q)$ est d'ordre $p + 1$.*

Démonstration — D'après le théorème 4.2.24, la courbe E est supersingulière si et seulement si l'entier $t = p + 1 - |E(\mathbb{F}_p)|$ est divisible par p, ce qui revient à affirmer que $|E(\mathbb{F}_p)|$ est congru à 1 modulo p. En utilisant la borne de Hasse, on en déduit que la seule possibilité est $|E(\mathbb{F}_p)| = p + 1$. □

Exemple 4.2.27 —

1. Considérons la courbe elliptique E sur $\mathbb{F}_q$ définie par l'équation
$$Y^2 = X^3 + X,$$
avec q congru à 3 modulo 4. Nous avons vu que $E(\mathbb{F}_q)$ est d'ordre $q + 1$. On en déduit que E est supoersingulière.
2. De même, pour la courbe elliptique E sur $\mathbb{F}_q$ définie par l'équation
$$Y^2 = X^3 - 1,$$
avec q congru à 2 modulo 3, le groupe $E(\mathbb{F}_q)$ est d'ordre $q + 1$, et E est supersingulière.

4.3. Applications en cryptographie

4.3.1. Le problème du logarithme discret elliptique — La loi de groupe sur une courbe elliptique étant de complexité polynomiale, il est naturel d'envisager des applications cryptographiques. Nous avons vu que le problème du logarithme discret sur les corps fini est difficile. Il n'existe en effet aucun algorithme pour le résoudre en temps polynomial. Cependant, les techniques les plus avancées permettent de le

résoudre en temps sub-exponentiel. Depuis les années 80, les cryptologues se sont intéressés au *problème du logarithme discret elliptique* : considérons une courbe elliptique E sur $\mathbb{F}_q$, et notons $G = \langle P \rangle$ le sous-groupe engendré par un pont $P \in E(\mathbb{F}_q)$. Soit n l'ordre de G. Étant donné $Q \in G$, on cherche à déterminer l'élément $m = \log_P(Q) \in \mathbb{Z}/n\mathbb{Z}$ tel que $Q = mP$. Dans la pratique, il apparaît que ce problème est en général très difficile, et il n'existe à ce jour aucun algorithme en temps sub-exponentiel permettant de le résoudre.

Remarque 4.3.1 — Bien qu'il n'existe aucun algorithme efficace permettant de résoudre le problème du logarithme discret elliptique dans le cas le plus général, sa résolution est cependant plus simple pour certaines classes particulières de courbes elliptiques. Par exemple, on peut montrer que le problème du logarithme discret sur une courbe elliptiques supersingulière définie sur $\mathbb{F}_q$ se réduit au problème du logarithme discret sur une extension finie de $\mathbb{F}_q$. La situation est encore plus particulière dans le cas d'une courbe E définie sur le corps premier $\mathbb{F}_p$ pour laquelle $E(\mathbb{F}_p)$ est d'ordre p, le problème pouvan être résolu en temps polynomial.

4.3.2. Le protocole de Diffie-Hellman — Les courbes elliptiques peuvent être utilisées pour implémenter les protocoles cryptographiques basés sur la difficulté de résolution du problème du logarithme discret. On obtient par exemple une version elliptique du protocole de Diffie-Hellman : voulant créer une clé secrète commune, Alice et Bob choisissent un corps fini $\mathbb{F}_q$, un courbe elliptique E sur $\mathbb{F}_q$ et un point $P \in E(\mathbb{F}_q)$ d'ordre n. Le couple (E, P) (ou le triplet $(\mathbb{F}_q, E, P)$) est public. Alice choisit un élément $a \in \mathbb{Z}/n\mathbb{Z}$ et transmet le point $Q = aP$. En procédant de la même manière, Bob choisit un secons élément $b \in \mathbb{Z}/n\mathbb{Z}$ et envoie l'élément $R = bP$. La clé commune est alors le point

$$S = abP = bQ = aR.$$

La connaissance de l'ordre n de P n'est pas vraiment nécessaire dans le déroulement du protocole. D'un point de vue pratique, il faut juste éviter que ses diviseurs premiers soient trop petits (l'algorithme de Silver, Pohlig et Hellman permettant alors de résoudre rapidement le problème du logarithme discret).

Remarque 4.3.2 — En utilisant l'*accouplement de Weil* sur une courbe elliptique E (qui est une forme bilinéaire sur E), Antoine Joux a développé un protocole d'échange de clé triparti permettant de créer une clé commune à trois participants.

4.3.3. Le cryptosystème El Gamal — Comme pour le protocole de Diffie-Hellman, il existe une version elliptique du cryptosystème El Gamal. Comme nous l'avions fait dans le cas des groupes multiplicatifs des corps finis, nous allons brièvement rappeler son principe, en le décrivant dans contexte des courbes elliptiques. Afin de recevoir des messages confidentiels par un canal non sécurisé, Alice procède de la manière suivante :

1. Elle choisit une courbe elliptique E sur un corps fini $\mathbb{F}_q$, un point $P \in E(\mathbb{F}_q)$ d'ordre n (grand) et un élément $a \in \mathbb{Z}/n\mathbb{Z}$, qui est sa clé secrète. La clé publique est le quadruplet $(\mathbb{F}_q, E, P, Q)$, avec $Q = aP$.
2. Afin d'envoyer le message $M \in E(\mathbb{F}_q)$, Bob choisit au hasard un élément $b \in \mathbb{Z}/n\mathbb{Z}$ et transmet à Alice le couple (R, S), avec $R = bP$ et $S = M + bQ$.
3. Afin de déchiffrer le cryptogramme (R, S), alice calcule $S - aR$. On a en effet les relations

$$S - aR = M + bQ - aR = M + abP - abP = M.$$