MAT 562 : Introduction à la géométrie algébrique et courbes elliptiques

Table des matières

Chapitre 1

Variétés algébriques affines et projectives

1.1 Généralités sur les anneaux. Anneaux de polynômes

Cette section donne une introduction et des rappels sur quelques propriétés des anneaux (commutatifs).

1.1.1 Idéaux

Soit A un anneau (commutatif). Le cas où A est **l'anneau** $k[x_1, \ldots, x_n]$ **des polynômes** en n variables sur un corps k nous est fondamental pour la suite.

Définition 1.1.1. Une partie $I \subset A$ est un **idéal** de A si I est un sous-groupe de A pour l'addition et si, pour tout $x \in I$ et tout $a \in A$, on a $ax \in I$.

Exemples :

1. $I = \{0\}, I = A$.
2. Pour $n \in \mathbb{Z}$ on définit $n\mathbb{Z} = \{x \in \mathbb{Z}, n \,|\, x\}$, qui est un idéal de $\mathbb{Z}$.
3. Si $S \subset A$ est une partie finie de A, on définit **l'idéal de** A **engendré par** S comme l'ensemble des sommes finies :
$$(S) = \{x = \sum_i s_i a_i, s_i \in S, a_i \in A\}.$$
4. Soient $I, J \subset A$ des idéaux dans A. On vérifie que les ensembles suivants sont des idéaux dans A :
   (a) $I + J = \{x + y, x \in I, y \in J\}$
   (b) $I \cdot J$ l'idéal engendré par $\{xy, x \in I, y \in J\}$;
   (c) $I \cap J = \{x \in A \,|\, x \in I \text{ et } x \in J\}$.

(d) Si $I \subset A$ est un idéal, on définit **le radical de** I

$$\sqrt{I} = \{a \in A \,|\, a^m \in I \text{ pour certain } m \geq 1\}.$$

On vérifie que $\sqrt{I}$ est un idéal de A.

Si $I \subset A$ est un idéal, considérons l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$. Cet ensemble, muni des opérations $\bar{a} + \bar{b} = \overline{a+b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$ forme un anneau, appelé **l'anneau quotient** A/I.

Exemples :

1. $k[x]/(x) \simeq k$;
2. $k[x, y]/(x) \simeq k[y]$;
3. la classe $\bar{x}$ dans $k[x]/(x^2)$ vérifie $\bar{x}^2 = 0$;
4. $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$;
5. si $f : A \to B$ est un homomorphisme surjectif d'anneaux, alors $I = ker(f)$ est un idéal de A et on a $A/I \simeq B$.

Définition 1.1.2. Un idéal I est **premier** si A/I est un anneau intègre. Un idéal I est **maximal** si A/I est un corps.

On a un énoncé suivant, dont la preuve découle du lemme de Zorn :

Théorème 1.1.3 (Krull). *Tout idéal $I \neq A$ d'un anneau A est inclus dans un idéal maximal.*

Dans le cas de l'anneau de polynômes sur un corps algébriquement clos on peut donner une liste exacte des idéaux maximaux :

Théorème 1.1.4. *Soit k un corps algébriquement clos. Tout idéal maximal $\mathfrak{m}$ de $k[x_1, \ldots, x_n]$ est de la forme $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ où $a_1, \ldots, a_n \in k$.*

On donnera la preuve de ce résultat à la fin de cette section.

1.1.2 Anneaux principaux, factoriels, noethériens.

Définition 1.1.5. Un anneau A est **principal** s'il est intègre et si tous ses idéaux sont de la forme $(x) = x\,A$ avec $x \in A$.

Exemples :

1. $\mathbb{Z}$;
2. $k[x]$ où k est un corps.

Pour A un anneau principal on a un analogue du théorème de Bézout :

Théorème 1.1.6. *Soit A un anneau principal. Soient $a, b \in A$. Alors a et b sont premiers entre eux si et seulement si $(a, b) = A$, i.e. s'il existe $u, v \in A$ tels que $ua + vb = 1$.*

Remarque. Par définition a et b sont premiers entre eux si pour tout $c \in A$ qui divise a (i.e. $a = ca'$ avec $a' \in A$) et qui divise b, on a que c est inversible.

La notion d'un anneau factoriel généralise la décomposition en facteurs premiers dans $\mathbb{Z}$.

Définition 1.1.7. Soit A un anneau et soit $p \in A$ un élément qui n'est pas inversible. On dit que p est **irréductible** si

$$p = ab \text{ avec } a, b \in A \Rightarrow a \text{ ou } b \text{ est inversible.}$$

Définition 1.1.8. Un anneau intègre A est dit **factoriel** si tout élément non nul $a \in A$ peut s'écrire de façon unique, à une permutation de facteurs et à une multiplication par des inversibles près, comme

$$a = up_1 \ldots, p_n,$$

où $u \in A$ est inversible et $p_1, \ldots p_n$ sont des éléments irréductibles.

Exemples et propriétés :

1. $\mathbb{Z}$ est factoriel ;
2. $k[x]$ est factoriel ;
3. plus généralement, un anneau principal est factoriel ;
4. si A est un anneau factoriel, alors l'anneau $A[x]$ est aussi factoriel (c'est un théorème assez difficile) ; en particulier, $k[x_1, \ldots, x_n]$ est factoriel.
5. Dans un anneau factoriel on a un analogue de *lemme de Gauss :* si A est un anneau factoriel, $a, b, c \in A$, alors on a
$$c \mid ab, (c, a) = 1 \Rightarrow c \mid b.$$
6. Dans un anneau factoriel A pour $p \in A$ irréductible l'idéal (p) est premier.

Définition 1.1.9. Soit A un anneau et soit M un A-module. On dit que M est **noethérien** si toute suite croissante $M_1 \subseteq M_2 \subseteq \dots M_n \subseteq \dots$ de sous-modules de M est stationnaire. Un anneau A est dit **noethérien** si A est noethérien en tant que A-module, i.e. si toute suite croissante $I_1 \subseteq I_2 \subseteq \dots I_n \subseteq \dots$ d'idéaux de A est stationnaire.

Proposition 1.1.10. *Un A-module M est noethérien si et seulement si tout sous-module de M peut être engendré par un nombre fini d'éléments. En particulier, un anneau A est noethérien si et seulement si tout idéal de A peut être engendré par un nombre fini d'éléments.*

La preuve est laissée en exercice.

Exemples :

1. Soit M un A-module. Si M est noethérien, alors tout sous A-module de M est noethérien, tout quotient de M est noethérien et tout module de type fini sur M est noethérien.
2. Un théorème de Hilbert dit que si A est un anneau noethérien, alors l'anneau $A[x]$ est aussi noethérien, en particulier, $k[x_1, \dots, x_n]$ est noethérien. Il résulte alors de l'exemple précédent que si B est une A-algèbre de type fini, alors B est un anneau noethérien : en effet, B est un quotient de $A[x_1, \dots x_n]$ (voir ci-dessous).
3. L'anneau $A = k[x_i]_{i\in\mathbb{N}}$ n'est pas noethérien. Le corps des fractions K de A, étant un corps, est noethérien. Ceci montre qu'un sous-anneau d'un anneau noethérien n'est pas nécessairement noethérien.

1.1.3 Notions de finitude

Définition 1.1.11. Soit K/k une extension de corps (non nécessairement finie). Soit $\alpha \in K$. On dit que α est **algébrique** sur k s'il existe un polynôme $P \in k[x]$ non nul, tel que $P(\alpha) = 0$. Dans le cas contraire on dit que α est **transcendant**.

Définition 1.1.12. Soit k un corps et soit A une k-algèbre. On dit que les éléments $a_1, \dots, a_m \in A$ sont **algébriquement indépendants** si pour tout polynôme $P \in k[x_1, \dots, x_m]$ la condition $P(a_1, \dots, a_m) = 0$ implique $P = 0$.

Définition 1.1.13. Soit A un anneau et soit B une A-algèbre. On dit que B est **de type fini** sur A si B est engendrée, en tant que A-algèbre, par un nombre fini d'éléments : $B \simeq A[x_1, \dots, x_n]$ (où les éléments $(x_i)_{1\leq i\leq n}$ ne sont pas nécessairement algébriquement indépendants). On dit que B est une A-algèbre **finie** si B est de type fini en tant qu'un A-module, i.e. B est engendrée par un nombre fini d'éléments en tant qu'un A-module : $B \simeq Ax_1 + \dots + Ax_n$.

Exemple.

1. Si k est un corps et $K = k(x)$ est une extension algébrique de k engendrée par x, alors K est un k-module de type fini. En effet, si $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ est un polynôme minimal de x, alors K est engendré par $1, x, \ldots x^{n-1}$.
2. Soit A un anneau. Si B est une A-algèbre de type fini (resp. finie) et C est une B-algèbre de type fini (resp. finie), alors C est une A-algèbre de type fini (resp. finie).

Proposition 1.1.14. *Soient $A \subseteq B \subseteq C$ des anneaux tels que*
(i) A est un anneau noethérien,
(ii) C est une A-algèbre de type fini,
(iii) C est un B-module de type fini.
Alors B est une A-algèbre de type fini.

Démonstration. Soient $x_1, \ldots, x_n$ les éléments de C qui engendrent C comme A-algèbre. Soient $y_1, \ldots, y_m \in C$ qui engendrent C comme B-module :

$$C = By_1 + \ldots + By_m.$$

On peut donc écrire, pour tous $1 \leq i, j \leq n$:

$$x_i = \sum_{t=1}^{m} b_{it} y_t$$

avec $b_{it} \in B$ et

$$y_i \cdot y_j = \sum_{t=1}^{m} c_{ijt} y_t.$$

Soit $B' \subset B$ un sous-anneau engendré sur A par les familles (b_{it}) et (c_{ijt}). Puisque B' est de type fini sur A et A est un anneau noethérien, on a que B' est noethérien (voir les exemples ci-dessus). Par construction, C est engendré par $y_1, \ldots y_m$ en tant que B'-module. On a donc que C, vu comme B'-module, est noethérien. Puisque B est un sous-module de C, on déduit que B est engendré par un nombre fini d'éléments, en tant que B'-module : $B = B'd_1 + \ldots + B'd_s$. On obtient que B est une A-algèbre de type fini, engendrée par les familles (b_{it}) et (c_{ijt}) et (d_i). □

Remarque 1.1.15. Dans le cas des k-algèbres, le *lemme de normalisation de Noether* (dont la preuve est nettement plus difficile) donne une structure plus précise : soit k un corps et soit A une k-algèbre de type fini. Alors il existe $y_1, \ldots y_n \in A$ algébriquement indépendants, tels que A est une $k[y_1, \ldots, y_n]$-algèbre finie.

Preuve du théorème 1.1.4. Soit $K = k[x_1, \ldots, x_n]/\mathfrak{m}$. L'énoncé du théorème est équivalent à

$$K = k[x_1, \ldots, x_n]/\mathfrak{m} \simeq k.$$

En effet, il suffit de prendre pour a_i l'image de x_i par l'isomorphisme ci-dessus.

Ensuite, puisque k est algébriquement clos, il suffit de montrer que K est algébrique sur k. Quitte à réordonner, on peut supposer que $x_1, \dots x_r \in K$ sont algébriquement indépendants sur k et que $x_{r+1}, \dots x_n$ sont algébriques sur $k(x_1, \dots, x_r)$, i.e. K est un $k(x_1, \dots, x_r)$-module de type fini. Si $r = 0$, le théorème est démontré. Supposons que $r > 0$.

D'après la proposition 1.1.14, appliquée à $B = k(x_1, \dots x_r)$, $C = K$ et $A = k$, B est une k-algèbre de type fini. On écrit

$$B = k[z_1, \dots, z_s]$$

avec

$$z_i = \frac{P_i(x_1, \dots x_r)}{Q_i(x_1, \dots x_r)}, P_i, Q_i \in k[x_1, \dots x_r].$$

Soit $f \in k[x_1, \dots, x_r]$ irréductible. On a $\frac{1}{f} \in B$. Comme $B = k[z_1, \dots z_s]$, on peut écrire $1/f$ comme un polynôme en z_i, en particulier, cela implique que f divise au moins un des Q_i. Or il n'y a qu'un nombre fini de polynômes qui vérifie cette propriété. Puisque k est algébriquement clos, il est en particulier infini. On a donc une famille infinie $(x - a)_{a \in k}$ de polynômes irréductibles sur k, contradiction. □

1.2 Variétés affines, Nullstellensatz

Soit k un corps. On identifie l'espace affine $\mathbb{A}^n_k$ avec l'ensemble k^n. Une variété algébrique affine sur k est une partie de k^n définie comme l'ensemble des zéros d'une famille de polynômes de $k[x_1, \dots, x_n]$:

Définition 1.2.1. Pour I un idéal de $k[x_1, \dots, x_n]$ on pose

$$V(I) = \{x = (x_1, \dots, x_n) \in k^n \mid f(x) = 0 \, \forall f \in I\}$$

la **variété algébrique affine** définie par I.

Si $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ est une famille finie de polynômes, on écrit $V(f_1, \dots, f_m)$ au lieu de $V((f_1, \dots, f_m))$. Notons que toute variété algébrique est de cette forme car l'anneau $k[x_1, \dots, x_n]$ est noethérien.

Les variétés affines que l'on considère en géométrie algébrique sont associées à des idéaux dans $k[x_1, \dots, x_n]$. On dit que X *est une variété algébrique affine* quand on considère une variété $X = V(I)$ et l'idéal I qui définit X ; *l'ensemble des points rationnels* $X(k) \subset k^n$ *d'une variété* X signifie que l'on considère une variété $X(k) = V(I)$ mais l'on oublie la donnée de I. Si K/k est une extension de k on écrit $X(K) = V(I_K) \subset K^n$ où $I_K \subset K[x_1, \dots, x_n]$ est un idéal engendré par I.

Notons que si k n'est pas algébriquement clos, alors l'ensemble $V(I)$ peut être vide : par exemple, pour $I = (x^2 + y^2 + 1) \subset \mathbb{R}[x, y]$. Si $k = \mathbb{C}$ et $I = (f)$ où $f \in k[x]$

est un polynôme non constant, le théorème fondamental d'algèbre dit que $V(I)$ est non vide. Dans le cas de polynômes en plusieurs variables, on a un énoncé analogue :

Théorème 1.2.2. [Nullstellensatz faible] *Soit k un corps algébriquement clos et soit I un idéal de $k[x_1, \ldots, x_n]$, $I \neq (1)$. Alors l'ensemble $V(I)$ est non vide.*

Démonstration. D'après le théorème de Krull, l'idéal I est contenu dans un idéal maximal $\mathfrak{m}$, qui est de la forme $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ d'après 1.1.4. On a $V(\mathfrak{m})$ est non vide, donc $V(I)$ est non vide lui aussi. □

Définition 1.2.3. Pour X un sous-ensemble de k^n on pose

$$I(X) = \{f \in k[x_1, \ldots, x_n],\ f(x) = 0\, \forall x \in X\}$$

l'idéal de X.

Notons que $I(X)$ est bien un idéal : si $f \in I(X)$ et $g \in k[x_1, \ldots, x_n]$, alors le polynôme fg s'annule en tout point de X.

Proposition 1.2.4. *1. Soient I, J des idéaux de $k[x_1, \ldots, x_n]$.*

(a) $I \subset J \Rightarrow V(J) \subset V(I)$;

(b) $V(I) \cap V(J) = V(I + J)$;

(c) $V(I) \cup V(J) = V(I \cdot J) = V(I \cap J)$.

2. Si $X \subset Y$ sont des sous-ensembles de k^n, alors $I(Y) \subset I(X)$.

3. Si J est un idéal de $k[x_1, \ldots, x_n]$, alors $J \subseteq I(V(J))$.

4. Si $X \subset k^n$ est une variété algébrique, alors $X = V(I(X))$.

Démonstration. Motrons *1(b)* et *1(c)*, les autres propriétés découlent immédiatement des définitions.

1(b). Soit $x \in V(I) \cap V(J)$. On a alors $f(x) = 0$ et $g(x) = 0$ pour tous $f \in I$ et $g \in J$. D'où $h(x) = 0$ pour tout $h \in I + J$. Inversement, si $h(x) = 0$ pour tout $h \in I + J$, on a en particulier que $f(x) = 0$ et $g(x) = 0$ pour tous $f \in I$ et $g \in J$, donc $x \in V(I) \cap V(J)$.

1(c). Soit $x \in V(I) \cup V(J)$. On a alors soit $f(x) = 0$ pour tout $f \in I$, soit $g(x) = 0$ pour tout $g \in J$. D'où $h(x) = 0$ pour tout $h \in I \cdot J$ (resp. pour tout $h \in I \cap J$). Inversement, supposons $h(x) = 0$ pour tout $h \in I \cdot J$ (resp. tout $h \in I \cap J$). Si $x \notin V(I)$, il existe $f \in V(I)$ tel que $f(x) \neq 0$. Soit $g \in J$. Comme $fg \in I \cdot J$ (resp. dans $I \cap J$), on déduit $g(x) = 0$. Donc $x \in V(J)$. □

D'après les propriétés précédentes, les ensembles $V(I)$ sont les fermés d'une topologie, dite **la topologie de Zariski** sur k^n. Si $X \subset k^n$ est une variété algébrique affine, on appelle la topologie induite sur X la **topologie de Zariski sur X.**

Notons qu'on n'a pas nécessairement d'égalité $J = I(V(J))$. En effet, on peut avoir deux types de problèmes :

1. si $J \neq \sqrt{J}$ (i.e. J n'est pas **radical**) : par exemple, pour $J = (x^2)$ un idéal dans $k[x]$, on a $I(V(J)) = (x)$;
2. si k n'est pas algébriquement clos : par exemple, pour $J = (x^2 + y^2)$ un idéal dans $\mathbb{R}[x, y]$, on a $I(V(J)) = (x, y)$.

Le théorème des zéros de Hilbert dit que ces deux problèmes sont essentiellement les seuls.

Théorème 1.2.5. [Nullstellensatz] *Soit k un corps algébriquement clos et soit J un idéal de $k[x_1, \ldots, x_n]$. Alors $I(V(J)) = \sqrt{J}$.*

Démonstration. On déduit le théorème de la version faible. Cet argument est dû à Artin et Tate. Soit $f \in I(V(J))$, i.e. f s'annule pour tous les zéros communs de J. Considérons l'idéal J' de $k[x_1, \ldots, x_{n+1}]$:

$$J' = (x_{n+1}f - 1, J).$$

On a alors $V(J') = \emptyset$. D'après Nullstellensatz faible, $1 \in J'$, autrement dit, on peut écrire dans l'anneau quotient $A = k[x_1, \ldots, x_{n+1}]/(x_{n+1}f - 1)$:

$$1 = \sum b_i a_i$$

avec $b_i \in J, a_i \in A$, d'où en regroupant les termes :

$$1 = c_0 + c_1 x_{n+1} + \ldots + c_m x_{n+1}^m$$

avec $c_i \in J$. Puisque $x_{m+1}f - 1 = 0$ dans A, cela donne

$$f^m = c_0 f^m + c_1 f^{m-1} + \ldots + c_m,$$

autrement dit, $f^m - c = 0$ où $c = c_0 f^m + c_1 f^{m-1} + \ldots + c_m \in J$. Puisque l'application naturelle $k[x_1, \ldots, x_n] \to A$ est injective, on déduit $f^m - c = 0$ dans $k[x_1, \ldots, x_n]$, d'où $f^m \in J$. □

Remarque 1.2.6. Notons que si $J = I(X)$, alors $J = \sqrt{J}$: si $f^m \in J$, alors $(f(x))^m = 0$ pour tout $x \in X$, d'où $f(x) = 0$ pour tout $x \in X$, i.e. $f \in J$.

On a donc introduit les objets de la catégorie des variétés algébriques affines sur un corps k. De façon générale, on s'intéresse aussi à comprendre les morphismes entre tels objets.

Définition 1.2.7. Soit X une variété algébrique dans k^n. Une **fonction polynomiale** sur X est une restriction d'une fonction dans $k[x_1, \ldots, x_n]$ à X. Si Y est une autre variété algébrique dans k^m, une application $f : X \to Y$ est **polynomiale** si

chacune des applications coordonnées l'est.

Notons qu'une fonction polynomiale $X \to Y$ est continue pour la topologie de Zariski : si $Z = V(I) \cap Y \subset Y$ est un fermé où I est un idéal de $k[y_1, \ldots, y_m]$ engendré par $(h_1, \ldots h_r)$, alors $f^{-1}(Z) = X \cap V(h_1 \circ f, \ldots h_r \circ f)$ est un fermé de X.

Proposition 1.2.8. *L'algèbre des fonctions polynomiales sur X est l'algèbre*

$$k[X] := k[x_1, \ldots, x_n]/I(X).$$

Démonstration. Soient $f, g \in k[x_1, \ldots, x_n]$ deux polynômes qui induisent les mêmes applications polynomiales sur X. On a donc $f - g = 0$ en tout point de X, d'où $f - g \in I(X)$. □

Soit $f : X \to Y$ une application polynomiale entre deux variétés affines définies sur un corps k. On définit une application $f^* : k[Y] \to k[X]$ par

$$f^*(\bar{P}) = \overline{P \circ f}$$

où $\bar{P}$ (resp. $\overline{P \circ f}$) est la classe de P (resp. $P \circ f$) dans $k[Y]$ (resp. $k[X]$). Cette application est effectivement bien définie : si $P_1 - P_2 \in I(Y)$ alors pour tout $x \in X$, on a $P_1(f(x)) = P_2(f(x))$ car $f(x) \in Y$.

Proposition 1.2.9. *Soient X, Y deux variétés affines. Soit $g : k[Y] \to k[X]$ un morphisme d'algèbres. Il existe une application polynomiale $f : X \to Y$ telle que $g = f^*$.*

Démonstration. On écrit $k[X] = k[x_1, \ldots, x_n]/I(X)$ et $k[Y] = k[y_1, \ldots, y_m]/I(Y)$ par la proposition précédente. Soit G le morphisme composé

$$k[y_1, \ldots, y_m] \to k[y_1, \ldots, y_m]/I(Y) \xrightarrow{g} k[x_1, \ldots, x_n]/I(X).$$

Soit $f_i = G(y_i)$. Soit $P_i \in k[x_1, \ldots, x_n]$ tel que $f_i = \bar{P}_i$. Posons $f = (P_1, \ldots, P_m)$. Car $f^*(\bar{y}_i) = \bar{P}_i = g(\bar{y}_i)$ par construction, il suffit de voir que f est à valeurs dans Y.

Soit $x = (a_1, \ldots, a_n) \in X$ et soit $h \in I(Y)$, on a

$$h(f(x)) = h(P_1(a_1, \ldots, a_n), \ldots, P_m(a_1, \ldots a_n)).$$

Pour tout $i = 1, \ldots, m$ on a que la valeur $P_i(a_1, \ldots, a_n)$ ne dépend que de la classe $\bar{P}_i$ de P_i dans $k[X]$. Comme $\bar{P}_i = G(y_i)$ on obtient

$$\begin{aligned} h(f(x)) &= h(G(y_1), \ldots, G(y_n))(a_1, \ldots, a_n) = \\ &= [G \text{ est un homomorphisme d'algèbres }] = Gh(y_1, \ldots y_m)(a_1, \ldots, a_n) = 0. \end{aligned}$$

donc $f(x) \in V(I(Y)) = Y$. □

Définition 1.2.10. Soit X une variété algébrique affine. On dit que X est **irréductible** si

$$X = X_1 \cup X_2,\ X_1, X_2 \text{ fermés de } X \Rightarrow X = X_1 \text{ ou } X = X_2.$$

Une variété X est irréductible si et seulement si l'idéal $I(X)$ est premier (voir les exercices). On a donc que l'anneau $k[X]$ est intègre. On appelle **le corps des fonctions** de X le corps des fractions $k(X)$ de l'anneau $k[X]$: les éléments de $k(X)$ sont des fractions f/g avec $f, g \in k[X]$ et $f/g = f_1/g_1$ si et seulement si $fg_1 = f_1 g$.

1.3 Exercices

1. Soit A un anneau. Montrer qu'un idéal I de A est maximal si et seulement si pour tout idéal J contenant I on a soit $J = I$, soit $J = A$.
2. Montrer qu'un anneau A est noethérien si et seulement si tout idéal de A peut être engendré par un nombre fini d'éléments.
3. Montrer que l'anneau $A = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[X]/(X^2 + 5)$ n'est pas factoriel.
4. Montrer que l'ensemble $X = \{(x, x) \in \mathbb{R}^2, x \neq 1\}$ n'est pas une variété algébrique affine dans $\mathbb{R}^2$.
5. Soit $J = \langle x^2 + y^2 - 1, y - 1 \rangle$.
   (a) Determiner $V(J)$.
   (b) Trouver une fonction $f \in I(V(J))$ telle que $f \notin J$.
   (c) Determiner $I(V(J))$.
6. Rappelons qu'un espace topologique X est dit irréductible si

$$X = F_1 \cup F_2,\ F_1, F_2 \text{ fermés de } X \Rightarrow F_1 = X \text{ ou } F_2 = X.$$

   (a) Montrer que X est irréductible si et seulement si pour tous $U_1, U_2 \subset X$ ouverts non vides, l'intersection $U_1 \cap U_2$ est non vide.
   (b) Montrer que X est irréductible si et seulement si tout ouvert U de X est dense dans X.
   (c) Montrer que si X est irréductible, alors tout ouvert non vide U de X est irréductible lui aussi.
   (d) Soit $X = V(I)$ une variété algebrique de k^n. Montrer que X, munie de la topologie de Zariski, est irréductible ssi $I(X)$ est premier.
   (e) Soit $X = V(I)$ une variété algebrique de k^n. Montrer que l'on peut écrire $X = X_1 \cup \ldots \cup X_m$ où X_i sont des variétés affines irréductibles, $X_i \not\subseteq X_j$ si $i \neq j$ et que cette écriture est unique à une permutation près.
   (f) Trouver les composantes irréductibles des variétés suivantes :
      i. $V(y, y^2 - xz) \subset \mathbb{A}^3_k$;

ii. $V(x(y-x^2+1), y(y-x^2+1)) \subset \mathbb{A}_k^2$.

iii. $V(x^2) \subset \mathbb{A}_k^2$

7. Soit $X = V(x^2 - yz, xz - x) \subset \mathbb{A}_k^3$. Trouver les composantes irréductibles de X et les idéaux qui définissent chacune de composantes.
8. Décrire l'ensemble $V(I)$ pour $I = (x^2 + y^2 - 1) \cap (y - 2 - x^2)$ un idéal de $k[x, y]$ dans le cas où $k = \mathbb{R}$ ou $\mathbb{C}$.
9. Montrer que le polynôme $f(x, y) = y^2 - x(x - 1)(x + 1) \in k[x, y]$ est irréductible sur tout corps. En déduire que $X = V(f)$ est irréductible. Faire un dessin dans le cas $k = \mathbb{R}$.
10. Soit k un corps algébriquement clos. Déterminer les idéaux $I(X)$ des variétés affines
    (a) $X = V(x^2y, (x - 1)(y + 1)^2)$;
    (b) $X = V(z - xy, y^2 + xz - x^2)$.
11. (a) Soit $f \in k[x, y]$ un polynôme irréductible. Montrer que le polynôme f, vu comme un polynôme en une variable y à coefficients dans $k(x)$ et un polynôme irréductible dans $k(x)[y]$.
    (b) Déterminer $I(X)$ pour $X = V(xy^3 + x^3y - x^2 + y)$.
12. (a) Soit $X = V(y - x^2)$. Montrer que $k[X]$ est isomorphe à l'anneau des polynômes en une variable.
    (b) Soit $X = V(xy - 1)$. Montrer que $k[X]$ n'est pas isomorphe à l'anneau des polynômes en une variable.
13. Soit k un corps qui n'est pas algébriquement clos.
    (a) Montrer qu'il existe un polynôme $f \in k[x, y]$ tel que $V(f) = (0, 0)$. En déduire par récurrence que pour tout $n > 0$ il existe un polynôme $F \in k[x_1, \ldots, x_n]$ tel que $V(F) = (0, \ldots, 0)$.
    (b) Si X est une variété affine sur k, montrer que X peut être définie par une seule équation.
14. Soit k un corps algébriquement clos.
    (a) Soient $f, g \in k[x, y]$ où f est un polynôme irréductible et g n'est pas divisible par f.
        i. Montrer qu'il existe $u, v \in k[x, y]$ et $h \in k[x] \setminus \{0\}$ tels que $uf + vg = h$.
        ii. En déduire que les courbes $V(f)$ et $V(g)$ ne s'intersectent qu'en un nombre fini de points.
    (b) Soit I un idéal premier de $k[x, y]$. Montrer que soit $I = (f)$ avec f un polynôme irréductible, soit I est maximal.
15. (**Groupes algébriques**) Soit k un corps algébriquement clos.
    (a) Montrer que le polynôme determinant $det(x_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}$ est un polynôme irréductible en n^2 variables.
    (b) Montrer que $GL_n(k)$ est un ouvert Zariski de $M_n(k) \simeq k^{n^2}$.

(c) Montrer que pour tout $0 \leq r \leq n$ l'ensemble M_r des matrices de rang au plus r est un fermé algébrique irréductible de M_k^n.

16. (a) Soient $V \subset k^n$ et $W \subset k^m$ deux variétés algébriques affines. Montrer que $X = V \times W$ est aussi une variété algébrique affine.

(b) Soit $\Delta \subset V \times V$ la diagonale donnée par $\Delta = \{(x, x), x \in V\}$. Montrer que Δ est une sous-variété fermée de $V \times V$. En déduire que la topologie de Zariski sur $V \times V$ n'est pas le produit de topologies de Zariski sur chacun des facteurs.

(c) Soient $p : X \to V$ et $q : X \to W$ deux projections. Montrer que p et q sont des applications polynomiales. Determiner les applications $p^* : k[V] \to k[X]$ et $q^* : k[W] \to k[X]$.

(d) Soit $Z \subset V \times \{w\} \subset V \times W$ un fermé. Montrer que la projection Z' de Z sur V est une sous-variété de V isomorphe à Z.

(e) Soient k un corps algébriquement clos, V, W deux variétés affines irréductibles. Montrer que le produit $V \times W$ est une variété irréductible.

Chapitre 2

Variétés projectives, courbes planes et courbes elliptiques

2.1 Variétés projectives

Soit k un corps. On peut voir l'espace projectif $\mathbb{P}_k^n$ comme l'ensemble des droites dans k^{n+1} qui passent par 0. Plus précisément, soit $\sim$ une relation d'équivalence sur k^{n+1} où l'on pose

$$x \sim y \text{ si et seulement si } x = \lambda y, \lambda \in k.$$

Définition 2.1.1. L'espace projectif $\mathbb{P}_k^n$ est défini comme le quotient

$$\mathbb{P}_k^n = k^{n+1} - \{0\}/\sim .$$

Pour $(x_0, \dots x_n) \in k^{n+1} - \{0\}$ on note $[x_0 : \dots : x_n]$ le point de $\mathbb{P}_k^n$ correspondant.

Si $f \in k[x_0, \dots, x_n]$ est un polynôme homogène de degré d, on a par définition $f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n)$. On définit alors les variétés projectives comme les lieux des zéros dans $\mathbb{P}_k^n$ de polynômes homogènes dans $k[x_0, \dots, x_n]$.

Définition 2.1.2. Un idéal I de $k[x_0, \dots, x_n]$ est **homogène** si $I = (f_1, \dots, f_m)$ où $f_i, 1 \leq i \leq m$ sont des polynômes homogènes.

On vérifie facilement que I est homogène si et seulement si pour tout $f \in I$ les composantes homogènes de f sont aussi dans I.

Définition 2.1.3. Pour I un idéal homogène de $k[x_0, \dots, x_n]$ on pose

$$V_p(I) = \{x = [x_0 : \dots : x_n] \in \mathbb{P}_k^n \mid f(x) = 0 \, \forall f \in I\}$$

la **variété algébrique projective** définie par I.

Définition 2.1.4. Pour X un sous-ensemble de $\mathbb{P}_k^n$ on pose

$$I_p(X) = \{f \in k[x_0, \ldots, x_n] \text{ homogène }, f(x) = 0 \, \forall x \in X\}$$

l'idéal de X.

Exemples.

1. **L'hyperplan** H dans $\mathbb{P}_k^n$ est défini comme le lieu des zéros d'une forme linéaire en $x_0, \ldots, x_n$:

   $$H = V_p(a_0 x_0 + \ldots + a_n x_n),$$

   où les coefficients $a_i \in k$ ne sont pas tous nuls.
2. Plus généralement, **l'hypersurface** de degré d dans $\mathbb{P}_k^n$ est définie comme le lieu des zéros d'un polynôme homogène de degré d en $x_0, \ldots, x_n$.
3. Si $V = V_p(I)$ une variété projective dans $\mathbb{P}_k^n$, on appelle le **cône** $C(V)$ de V la variété affine dans $\mathbb{A}_k^{n+1}$ définie par $C(V) = V(I)$. On vérifie que $I_p(V) = I(C(V))$.

De même comme dans le cas affine, on a les propriétés suivantes :

Proposition 2.1.5. *1. Soient I, J des idéaux homogènes de $k[x_0, \ldots, x_n]$. On a $I \subset J \Rightarrow V_p(J) \subset V_p(I)$.*

2. Si $X \subset Y$ sont des sous-ensembles de $\mathbb{P}_k^n$, alors $I_p(Y) \subset I_p(X)$.

3. Si $X \subset \mathbb{P}_k^n$ est une variété algébrique, alors $X = V_p(I_p(X))$.

4. Si J est un idéal homogène de $k[x_0, \ldots, x_n]$, alors $J \subseteq I_p(V_p(J))$.

5. Si k est infini et $V = V(I)$ est une variété projective dans $\mathbb{P}_k^n$, alors $I_p(V) = I(C(V))$.

Démonstration. Montrons la dernière propriété, les autres sont analogues au cas affine. L'inclusion $I_p(V) \subseteq I(C(V))$ est évidente. Soit $f \in I(C(V))$. Écrivons $f = \sum f_d \in k[x_0, \ldots, x_n]$ où les f_d sont les composantes homogènes de f. Puisque V est une variété projective, si $(x_0, \ldots, x_n) \in C(V)$, alors pour tout $\lambda \in k$ on a $(\lambda x_0, \ldots, \lambda x_n) \in C(V)$, i.e. le polynôme

$$g(\lambda) = f(\lambda x_0, \ldots, \lambda x_n) = \sum \lambda^d f_d(x_0, \ldots, x_n)$$

s'annule en tout $\lambda \in k$. Puisque k est infini, $f_d(x_0, \ldots, x_n) = 0$ pour tout d, i.e. les composantes homogènes de f sont dans $I(C(V))$, d'où $I(C(V)) \subseteq I_p(V)$. □

Cartes affines de $\mathbb{P}_k^n$. Soit $\phi_i : \mathbb{A}_k^n \to \mathbb{P}_k^n, i = 0, \ldots, n$ le morphisme $(x_1, \ldots, x_n) \mapsto (x_1 : \ldots : x_{i-1} : 1 : x_i : \ldots x_n)$. Il est clair que l'espace $\mathbb{P}_k^n$ est recouvert par les images des applications ϕ_i. Par ailleurs, soit $U_i \subset \mathbb{P}_k^n$ l'ouvert $\{x_i \neq 0\}$: c'est le complémentaire de l'hyperplan $x_i = 0$. Soit

$$\psi_i : U_i \to \mathbb{A}_n^k, (x_0 : \ldots : x_n) \mapsto (\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}.)$$

On voit immédiatement que ψ_i est un isomorphisme, dont l'inverse est l'application ϕ_i. On appelle alors U_i les **cartes affines** de $\mathbb{P}_k^n$.

Un polynôme homogène $f(x_0, \ldots, x_n)$ de degré d induit une application polynomiale f_i sur U_i donnée par $f_i(x_0, \ldots, x_{i-1}, 1, x_{i+1}, x_n)$. Inversement, si $f \in k[x_1, \ldots x_n]$ un polynôme de degré d, on appelle la **homogénisation** de f le polynôme homogène

$$f^*(x_0, \ldots, x_n) = x_0^d f(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}).$$

On peut bien sûr faire une construction analogue avec x_i à la place de x_0.

Si I est un idéal homogène dans $k[x_0, \ldots x_n]$, on s'intéresse aussi à savoir si $V_p(I)$ est non vide. Il est clair que cela n'est pas le cas si $I = (x_0, \ldots, x_n)$ ou même si $I = (x_0^r, \ldots, x_n^r)$. Une version projective du théorème de Hilbert des zéros dit que sur un corps algébriquement clos ce sont les seuls tels exemples :

Théorème 2.1.6 (**Nullstellensatz homogène**). *Soit k un corps algébriquement clos et soit I un idéal homogène de $k[x_0, \ldots, x_n]$.*
(i) $V_p(I) = \emptyset \Leftrightarrow \exists r > 0,\ (x_0, \ldots, x_n)^r \subset I$;
(ii) si $V_p(I) \neq \emptyset$, alors $I_p(V_p(I)) = \sqrt{I}$.

Démonstration. (i) L'implication $\Leftarrow$ est immédiate. Montrons l'implication $\Rightarrow$. On a $V_p(I) = \emptyset \Leftrightarrow C(V) = \{(0, \ldots, 0) \in k^{n+1}\}$. D'après le Nullstellensatz affine, cela est équivalent à dire que $\sqrt{I} = (x_1, \ldots, x_n)$, ce qui implique que $\exists r > 0,\ (x_0, \ldots, x_n)^r \subset I$.
(ii) Si $V_p(I) \neq \emptyset$, on a $I_p(V) = I(C(V)) = \sqrt{I}$ par 2.1.5 et par le Nullstellensatz affine.

□

Exemples de morphismes. Soit $(f_0, \ldots f_m)$ une famille d'applications polynomiales homogènes de degré d en n variables $x_0, \ldots, x_n$, à coefficients dans un corps k. Si les polynômes f_i n'ont pas de zéros communs $(x_0, \ldots, x_n) \neq (0, \ldots, 0)$ (si k est algébriquement clos, cela revient à dire que l'idéal $(x_0, \ldots, x_n)^r$ est contenu dans l'idéal engendré par $f_1, \ldots, f_m$), alors on peut définir une application

$$F : \mathbb{P}_k^n \to \mathbb{P}_k^m, (x_0 : \ldots : x_n) \mapsto (f_0(x_0 : \ldots x_n), \ldots : f_m(x_0, \ldots x_n)).$$

Plus généralement, soient $X \subset \mathbb{P}_k^n$ et $Y \subset \mathbb{P}_k^m$ deux variétés projectives. Si $X \cap V(f_0, \ldots f_m) = \emptyset$ et si pour tout $x \in X$ on a $(f_0(x), \ldots, f_m(x)) \in Y$, alors on peut définir une application

$$F : X \to Y, (x_0 : \ldots : x_n) \mapsto (f_0(x_0, \ldots x_n) : \ldots : f_m(x_0, \ldots x_n)).$$

Exemples :

1. Soit $V \subset \mathbb{P}^2_k$ une hypersurface de degré 2 (une conique) donnée par l'équation $x^2+y^2-z^2=0$. On a un morphisme $\mathbb{P}^1 \to V, (u:v) \mapsto (u^2-v^2, 2uv, u^2+v^2)$.
2. Soit $k=\mathbb{F}_q$ un corps fini et soit $V \subset \mathbb{P}^n_k$ une variété projective. On définit le morphisme de Frobenius par $Fr : V \to V, (x_0 : \ldots : x_n) \mapsto (x_0^q : \ldots : x_n^q)$.
3. Soit $P = (0 : \ldots : 0 : 1) \in \mathbb{P}^n_k$. Une droite $L \subset \mathbb{P}^n_k$ qui passe par le point P est l'image d'un morphisme $\mathbb{P}^1_k \to \mathbb{P}^n_k$, $[u:v] \mapsto (a_0u : a_1u \ldots : a_{n-1}u : v)$, elle est donc déterminée par la donnée de $(a_0 : \ldots : a_{n-1})$. L'ensemble des droites dans $\mathbb{P}^n_k$ qui passent par un point donné est donc l'espace projectif de dimension $n-1$.

Dans ce cours on va considérer des variétés affines, projectives ou leurs produits. Une motivation pour s'intéresser à des variétés projectives (plutôt qu'à des variétés affines) est le théorème suivant qui permet de donner le nombre exact de points d'interesection de deux courbes dans le plan projectif (ce qui n'est pas vérifié dans le cas de $\mathbb{A}^2_k$ car on peut par exemple avoir deux droites parallèles.)

Théorème 2.1.7 (Théorème de Bézout)**.** *Soient k un corps algébriquement clos et C_1, C_2 deux courbes projectives définies par des équations homogènes de degrés d_1 et d_2 dans $\mathbb{P}^2_k$. Alors le nombre de points d'intersection de C_1 et C_2 comptés avec les multiplicités, est égal à d_1d_2.*

Dans la suite nous verrons la preuve de ce théoréme dans le cas où C_1 est une droite ou une conique. Ces deux cas sont utilisés pour définir la loi de groupe sur les points d'une courbe elliptique.

2.2 Courbes elliptiques : premières propriétés

Une image. Supposons qu'on a une pyramide formée de n boules. Si la pyramide s'écrase, peut-on arranger les boules dans un carré ?

Si l'on note x la hauteur de la pyramide, on voit facilement que l'on cherche des solutions entières de l'équation $y^2 = x(x+1)(2x+1)/6$. Cette équation définit une courbe élliptique. On peut montrer que les seules solutions entières sont $(1,1)$ et $(24,70)$.

Soient k un corps et $C \subset \mathbb{P}^2_k$ une courbe plane définie par une équation homogène $F(X,Y,Z)=0$.

Définition 2.2.1. La courbe C est **lisse** en un point $P \in C$ si

$$(\partial F/\partial X(P), \partial F/\partial Y(P), \partial F/\partial Z(P)) \neq (0,0,0).$$

Si c'est le cas, la droite tangente à C au point P est la droite

$$\frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z = 0.$$

La courbe C est **lisse** si elle est lisse en tout point.

De manière générale, on définit une courbe elliptique comme une courbe plane lisse E définie par une équation homogène de degré 3 et qui admet un point : $E(k) \neq \emptyset$. On peut montrer qu'une telle courbe peut être définie par l'équation suivante, dite **la forme de Wierstrass** de E, ce que l'on prendra comme définition pour ce cours.

Définition 2.2.2. Une **courbe elliptique** E est une courbe plane définie par une équation

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \text{ avec } 4a^3 + 27b^2 \neq 0. \tag{2.1}$$

On a effectivement que $E(k) \neq \emptyset$. Le point $O_E = (0 : 1 : 0)$ est dans E. On appelle $\Delta = -(4a^3 + 27b^2)$ le **discriminant** de E.
Suivant le contexte, on appelle aussi **courbe elliptique** une courbe affine définie par une équation

$$y^2 = x^3 + ax + b \tag{2.2}$$

avec les mêmes conditions sur a et b. C'est l'ouvert $\{Z \neq 0\}$ de la courbe donnée par l'équation (2.1). Le complémentaire de cet ouvert ne contient qu'un seul point O_E. Les conditions sur a et b sont justifiées par le lemme suivant :

Lemme 2.2.3. *(i) La courbe plane C définie par une équation $Y^2Z = X^3 + aXZ^2 + bZ^3$ est lisse si et seulement si $\Delta = -(4a^3 + 27b^2) \neq 0$.*
(ii) Soient e_1, e_2, e_3 les racines de $f(x) = x^3 + ax + b$ dans une clôture algébrique $\bar{k}$ de k : $f(x) = (x - e_1)(x - e_2)(x - e_3)$. Alors

$$\Delta = [(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)]^2.$$

Démonstration. Laissée en exercice. □

Pour P un point d'une courbe elliptique E on écrit $P = (X_P : Y_P : Z_P)$ dans les coordonnées projectives (2.1) ou $P = (x_P, y_P)$ dans les coordonnées affines (2.2), si $P \neq O_E$. Le résultat fondamental dans la théorie des courbes elliptiques est que les points d'une courbe elliptique forment un groupe abélien. Cela est aussi la base pour des applications cryptographiques.

La loi de groupe : définition. Soit E une courbe elliptique donnée par une équation affine (2.2). Soient $P \neq Q \in E(k)$. Puisque E est définie par une équation de degré 3, la droite L coupe E en troisième point R (cf. lemme 2.3.1 et la remarque après), eventuellement $R = O_E$. On pose $P + Q = -R$ où le point $-R$ est le point $(X_R : -Y_R : Z_R)$. Si $P = Q$ on prend pour L la droite tangente en P. On pose également $P + O_E = O_E + P$, $O_E + O_E = O_E$.

Théorème 2.2.4. *L'ensemble $E(k)$ muni de la loi ci-dessus forme un groupe abélien avec l'élément neutre O_E.*

Démonstration. D'après la définition, il est évident que la loi ci-dessus est commutative, admet l'élément neutre O_E et pour out P on a l'inverse $-P$. On démontre l'associativité dans la section suivante, pour ce faire on aura besoin de quelques résultats de la géométrie projective. □

On peut aussi décrire explicitement les formules de la loi de groupe sur une courbe elliptique :

Proposition 2.2.5. *Soient $P, Q \in E(k)$ les points distincts de O_E.*

1. $-P = (x_P, -y_P)$;
2. *Si $P = Q$ soit $\lambda = (3x_P^2 + a)/2y_P$ et $\mu = y_P - \lambda x_P$. Alors*
$$P + Q = (\lambda^2 - x_P - x_Q, -\lambda^3 + \lambda(x_P + x_Q) - \mu).$$
3. *Si $P \neq Q$ soit $\lambda = \frac{y_P - y_Q}{x_P - x_Q}$ et $\mu = y_P - \lambda x_P$. Alors $\lambda = \frac{x_P^2 + x_P x_Q + x_Q^2 + a}{y_P + y_Q}$ et*
$$P + Q = (\lambda^2 - x_P - x_Q, -\lambda^3 + \lambda(x_P + x_Q) - \mu).$$

Démonstration. L'expression de $-P$ est immédiate d'après la définition. Soit L la droite PQ si $P \neq Q$ et la droite tangente à E en P, si $P = Q$. D'après la définition de λ et μ, la droite L est donnée par l'équation $y = \lambda x + \mu$. Soit R le troisième point d'intersection de la droite L avec la courbe E. On a $P + Q = (x_R, -y_R)$. La coordonnée du point R est une solution de

$$0 = x^3 + ax + b - (\lambda x + \mu)^2 = x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + (b - \mu^2).$$

Puisque x_P et x_Q vérifient cette équation, on déduit les expressions de la troisième solution comme dans l'énoncé. □

Les formules suivantes nous séront utilles pour la suite :

Proposition 2.2.6.

1. $x_{P+Q} + x_{P-Q} = \frac{2(x_P + x_Q)(a + x_P x_Q) + 4b}{(x_P - x_Q)^2}$.
2. $x_{P+Q} x_{P-Q} = \frac{(x_P x_Q - a)^2 - 4b(x_P + x_Q)}{(x_P - x_Q)^2}$.
3. $x_{2P} = \frac{x_P^4 - 2ax_P^2 - 8bx_P + a^2}{4(x_P^3 + ax_P + b)}$.

Démonstration. On vérifie les identités de la proposition en utilisant les formules explicites pour la loi de groupe 2.2.5. □

2.3 Un peu de géométrie projective et l'associativité de la loi de groupe

Dans cette section k est un corps algébriquement clos. On commence par démontrer les deux premiers cas du théorème de Bézout.

Lemme 2.3.1. *Soit $C \subset \mathbb{P}^2_k$ une courbe définie par un polynôme homogène de degré d et soit $L \subset \mathbb{P}^2_k$ une droite ne pas contenue dans C (en tant qu'une composante). Alors $C \cap L$ est composé de d points comptés avec multiplicités.*

Démonstration. Soient $F(X, Y, Z) = 0$ l'équation homogène de degré d qui définit la courbe C et $aX + bY + cZ = 0$ l'équation de la droite L. Quitte à permuter les coordonnées, on peut supposer que $a \neq 0$ et que l'équation de la droite est donc $X = -b'Y - c'Z$. Le polynôme $f(Y, Z) = F(-b'Y - c'Z, Y, Z)$ est un polynôme homogène non nul (car L n'est pas contenue dans C) de degré d. Comme k est algébriquement clos, on a donc une factorisation

$$f(Y, Z) = \alpha(Y - \alpha_i Z)^{m_i} \tag{2.3}$$

avec $\sum m_i = d$. Les points d'intersection de L et C sont donnés par la condition $f(Y, Z) = 0$, on a donc $\sum m_i = d$ de tels points. □

Remarque. Supposons que k n'est pas algébriquement clos. Si C, L et $d - 1$ points d'intersections de L et C sont définis sur k, alors dans la démonstration ci-dessus $f(Y, Z)$ admet un facteur de degré $d - 1$ défini sur k. On a donc que la décomposition (2.3) vaut sur k et tous les d points d'intersection de L et C sont définis sur k.

Lemme 2.3.2. *Soit $C \subset \mathbb{P}^2_k$ une courbe définie par un polynôme homogène de degré d et soit $D \subset \mathbb{P}^2_k$ une conique non pas contenue dans C. Alors $C \cap D$ est composé de $2d$ points comptés avec multiplicités.*

Démonstration. Soit $F(X, Y, Z) = 0$ l'équation homogène de degré d qui définit la courbe C. Si la conique D est réductible, D est l'union de deux droites et l'énoncé découle du lemme précédent (voir l'exercice 1). Quitte à faire un changement linéaire en coordonnées, on peut supposer que la conique est donnée par l'équation $XY - Z^2 = 0$, i.e. que D est l'image de morphisme $\mathbb{P}^1 \to \mathbb{P}^2, (u : v) \mapsto (u^2 : v^2 : uv)$ (voir l'exercice 1). Le polynôme $f(u, v) = F(u^2, v^2, uv)$ est un polynôme homogène non nul (car D n'est pas contenue dans C) de degré $2d$. Comme k est algébriquement clos, on a donc une factorisation $f(Y, Z) = \alpha(Y - \alpha_i Z)^{m_i}$ avec $\sum m_i = 2d$. Les points d'intersection de D et C sont donnés par la condition $f(u, v) = 0$, on a donc $\sum m_i = 2d$ de tels points. □

Dans les énoncés suivants on s'intéresse à décrire les courbes de degré donné qui passent par un certain nombre de points donnés. De façon générale, l'ensemble des hypersurfaces de degré d dans $\mathbb{P}^N_k$ forme aussi un espace projectif, dont les coordonnées correspondent à des coefficients. Par exemple, une conique dans $\mathbb{P}^2_k$ est donnée par une équation homogène $q(X, Y, Z) = \sum a_{ijs} X^i Y^j Z^s$ avec $i + j + s = 2$, on a donc 6 coefficients possibles. On associe à la conique le vecteur de ces coefficients. L'ensemble de toutes les formes $q(X, Y, Z)$ forme donc un espace vectoriel de dimension 6. Deux formes définisssent la même conique si elles ne se distinguent

que par multiplication par un scalaire. L'ensemble des coniques est donc un espace projectif $\mathbb{P}^5_k$.

Lemme 2.3.3. *Soient $P_1, \ldots, P_5$ des points distincts de $\mathbb{P}^2_k$. Il existe une conique dans $\mathbb{P}^2_k$ qui passe par ces points. De plus, si quatre de ces points ne sont jamais alignés, la conique est unique.*

Démonstration. Une conique C dans $\mathbb{P}^2_k$ est donnée par une équation homogène $q(X,Y,Z) = \sum a_{ijs} X^i Y^j Z^s$ avec $i+j+s = 2$. Le k-espace vectoriel V des coefficients d'une conique est donc de dimendion 6. La condition que la conique C de passe par un point donne une condition linéaire dans cet espace. Les coefficients d'une conique qui passe par 5 points sont donc les solutions d'un système de 5 équations linéaires dans un espace de dimension 6. On a donc toujours une conique qui passe par 5 points.

Supposons que 3 points, disons P_1, P_2, P_3 sont alignés. Soit L la droite P_1P_2. L'équation q de la conique C est donc divisible par l'équation de L et q s'annule en P_4 et P_5. Comme P_4 et P_5 ne sont pas sur L, la conique C est l'union de deux droites $L \cup P_4P_5$.

Supposons qu'aucun triplet des points $P_1, \ldots, P_5$ n'est aligné. Soit P_6 un point sur la droite $L = P_1P_2$, différent de P_1 et de P_2. Supposons que la dimension de k-espace vectoriel des équations des coniques qui passent par des points $P_1, \ldots, P_5$ est au moins 2. Il existe alors une conique contenant $P_1, \ldots, P_6$, car la condition qu'une conique passe par un point donné est une condition linéaire. Puisque P_1, P_2, P_6 sont alignés, C est l'union de L et une autre droite, on a donc que $P_3, \ldots, P_5$ alignés, contradiction. □

Lemme 2.3.4. *Soient $P_1, \ldots, P_8$ des points distincts de $\mathbb{P}^2_k$, tels que quatre d'entre eux ne sont jamais alignés et que sept d'entre eux n'appartiennent jamais à la même conique. Soit V le k-espace vectoriel des polynômes homogènes de degré 3 s'annulant en $P_1, \ldots, P_8$. Alors* $\dim V = 2$.

Démonstration. Le k-espace vectoriel W des coefficients d'une cubique est de dimension 10, ainsi $\dim V \geq 10 - 8 = 2$. On a les cas suivants à considérer :

1. Supposons que P_1, P_2, P_3 sont alignés, soit L la droite correspondante. Soit P_9 un point (distinct de P_1, P_2, P_3) sur cette droite. L'espace vectoriel des cubiques qui passent par ces neuf points est de dimension $\dim V - 1$. Si une cubique C passe par $P_1, \ldots, P_9$, alors l'intersection de C et L contient au moins 4 points et C est donc de la forme $L \cup Q$ pour Q une conique. D'après les hypothèses, Q contient $P_4, \ldots, P_8$. D'après le lemme 2.3.3, il n'existe qu'une seule telle conique. Ainsi $\dim V - 1 \leq 1$, d'où le résultat.
2. Supposons que $P_1, P_2, \ldots, P_6$ sont sur une conique Q. Soit P_9 un autre point sur cette conique. On a encore que toute cubique qui contient $P_1, \ldots P_9$ doit contenir Q et s'écrit donc comme $C = Q \cup L$. D'après les hypothèses, $L = P_7P_8$. On a donc encore $\dim V - 1 \leq 1$, d'où le résultat.

3. Cas général : trois points parmi $P_1, \ldots, P_8$ sont jamais alignés, six points sont jamais sur une conique. Soient P_9, P_{10} sur la droite $L = P_1P_2$ différents de P_1 et P_2. Supposons $\dim V > 2$. Il existe alors une cubique C qui passe par $P_1, \ldots, P_{10}$, cette cubique contient donc la droite L et elle est donc l'union de L est d'une conique. On obtient une contradiction avec les hypothéses sur $P_1, \ldots, P_8$.

□

Lemme 2.3.5. *Soient C_1 et C_2 deux cubiques dans $\mathbb{P}^2_k$. Supposons que C_1 est irréductible. Supposons qu'on a neuf points $P_1, \ldots P_9$ d'intersection de C_1 et C_2, tels que les points $P_1, \ldots, P_8$ sont distincts. Si une cubique C passe par les points $P_1, \ldots, P_8$, alors elle passe par le point P_9.*

Démonstration. La cubique C_1 ne contient pas 4 points alignés : d'après le lemme 2.3.1, on aurait que C_1 contient une droite, ce qui n'est pas possible car C_1 est irréductible. De même, C_1 ne contient pas 7 points sur une conique. Les points $P_1, \ldots, P_8$ satisfont donc les hypothèses du lemme 2.3.4 et le k-espace vectoriel des polynômes homogènes de degré 3 s'annulant en $P_1, \ldots, P_8$ est de dimension 2. Il est donc engendré par C_1 et C_2. Ainsi, l'équation de la cubique C est une combinaison linéaire des équations de C_1 et C_2, en particulier, elle s'annule en P. □

La loi de groupe sur une courbe elliptique

Associativité de la loi de groupe : cas général.

On prend $P, Q, R \in E(k)$ trois points distincts. On pose
L_1 est la droite PQ, T est le troisième point d'intersection avec E ;
L_2 est la droite TO_E, $T' = -T$ est le troisième point d'intersection avec E ;
L_3 est la droite RT', U est le troisième point d'intersection avec E ;
M_1 est la droite QR, S est le troisième point d'intersection avec E ;
M_2 est la droite SO_E, $S' = -S$ est le troisième point d'intersection avec E ;
M_3 est la droite PS', V est le troisième point d'intersection avec E ;
D'après la construction, $(P + Q) + R = -U$ et $P + (Q + R) = -V$ et on veut donc montrer que $U = V$.

Soient $C_1 = L_1 + M_2 + L_3$ et $C_2 = M_1 + L_2 + M_3$ deux cubiques. On a $E \cap C_1 = \{P, Q, R, O_E, T, T', S, S', U\}$ et $E \cap C_2 = \{P, Q, R, O_E, T, T', S, S', V\}$. Supposons que les points $P, Q, R, O_E, T, T', S, S', U$ sont tous distincts. D'après le lemme 2.3.5 pour E et C_1, on a alors $U = V$. Les cas qui restent sont démontrés ci-dessous, en utilisant la loi de groupe explicite.

Associativité de la loi de groupe : fin de la preuve. Dans les notations du cas général, on a démontré l'associativité de la loi de groupe dans le cas où les points $P, Q, R, O_E, T, T', S, S'$ sont tous distincts. Pour finir la démonstration, il nous reste à étudier les cas suivants :

1. Un au moins parmi les points $P, Q, R, T, T', S, S', U, V$ est le point O_E.
   (a) Si $O_E \in \{P, Q, R\}$, on a $(P+Q)+R = P+(Q+R)$ d'après la définition de l'addition avec O_E.
   (b) Supposons qu'aucun des points P, Q, R n'est le point O_E. D'après la construction, $T = O_E$ ssi $T' = O_E$. Supposons que c'est le cas. On a donc $Q = -P$. Il s'agit de montrer que $R = (P+(-P))+R = P+((-P)+R)$, ce qui est clair d'après la définition et un argument de symétrie par rapport à l'axe $y = 0$. En effet, soient D la droite qui passe par les points $-P$ et R, et K le troisième point d'intersection de D avec E. On a alors $-P+R = -K$. La droite D' qui passe par les points P et $-K$ est symétrique à D par rapport à l'axe $y = 0$. Le troisième point d'intersection de D' et E est donc le point $-R$, ce qui montre que $P+(-K) = R$, ce qu'il fallait démontrer. On vérifie de même le cas $S = O_E$. Notons que ce cas implique aussi que pour deux points W et W_1 de E on a

$$W = W_1 \Leftrightarrow (-P)+W = (-P)+W_1.$$

      En effet, l'impication $\Rightarrow$ est évidente et pour l'implication $\Leftarrow$ on observe que $P+((-P)+W) = (P+(-P))+W = W$, et de même pour W_1.
   (c) Supposons que $U = O_E$, i.e. que $R = -(P+Q)$. Il s'agit de montrer que

$$(P+Q)+(-(P+Q)) = P+(Q+(-(P+Q))).$$

      La partie gauche vaut O_E. On a donc

$$O_E = P+(Q+(-(P+Q))) \Leftrightarrow -P = Q+(-(P+Q)) \Leftrightarrow -P+(-Q) = -(P+Q),$$

      ce qui est immédiat par un argument de symétrie. Le cas $V = O_E$ est analogue.
2. Supposons que

   (*) $O_E \notin \{P, Q, R, T, T', S, S', U, V\}$ et qu'aucune des paires $(P, Q), (Q, R), (P+Q, R), (P, Q+R)$ ne contient deux points égaux.

   Soit E^0 l'ouvert affine $E \setminus \{O_E\}$ de la courbe E et soit A la variété affine $E^0 \times E^0 \times E^0$. D'après l'exercice 16 de chapitre 1, la variété A est irréductible et tout ouvert de A est irréductible. Soit $A' \subset A$ l'ouvert $\{P \neq Q, P \neq -Q, Q \neq R, Q \neq -R\}$. D'après les formules de la loi explicite, pour tout $(P, Q, R) \in A'$, les coordonnées des points $P+Q$ et $Q+R$ sont données par les formules 2.2.5.3, en particulier $x_{P+Q} = f(x_P, x_Q, y_P, y_Q)$ où $f = f_1/f_2$ est une fraction rationnelle avec le dénominateur non nul, de même pour $y_{P+Q} = g_1/g_2$. La condition $P+Q = R$ est donc donnée par des conditions polynomiales $f_1 - x_R f_2 = 0$, $g_1 - y_R g_2 = 0$. On a de même pour la condition $P = Q+R$. On en déduit que le lieu des points $(P, Q, R) \in A'$ où la condition $(*)$ est vérifiée est un ouvert A'' de A'. Par le même argument que ci-dessus, pour tout $(P, Q, R) \in A''$, on exprime les coordonnées des points

$P+Q, (P+Q)+R, Q+R, P+(Q+R)$ via les formules 2.2.5.3, en particulier, le lieu des points $(P,Q,R) \in A''$ tels que $(P+Q)+R = P+(Q+R)$ est un fermé B de A''. Or ce fermé contient un ouvert correspondant au cas général, où tous les points $P, Q, R, T = -(P+Q), T' = (P+Q), S = -(Q+R), S' = (Q+R), O_E, U = -((P+Q)+R)$ sont distincts. Puisque A'' est irréductible, tout ouvert est dense, et donc $B = A''$, ce qui montre que pour tous (P,Q,R) satisfaisant $(*)$ on a $(P+Q)+R = P+(Q+R)$.

3. Le cas où les points $P, Q, R, P+Q, Q+R$ ne sont pas tous distincts et aucun parmi les points $P, Q, R, T, T', S, S', U, V$ n'est le point O_E est laissé en exerice.

□

2.4 Exercices

1. Soit k un corps algébriquement clos et soit $q(X,Y,Z)$ une forme quadratique en trois variables. Soit $Q = V_p(q) \subset \mathbb{P}^2_k$. Montrer que soit Q est l'union de deux droites, soit Q est une conique irréductible qui peut être déinie par une équation $XY - Z^2$, quitte à faire un changement linéaire en coordonnées.
2. (**Quadriques**) Soit k un corps. Soit $X \subset \mathbb{P}^n_k$ une quadrique : X est une variété projective définie par une forme homogène $q(x_0, \ldots, x_n)$ de degré 2. Supposons que X est lisse : pour tout point $P = (x_0, \ldots x_n) \in X$ l'une au moins des dérivées $\partial q/\partial x_i(P)$ est non nulle, dans ce cas le plan tangent à X en P est donné par l'équation $\sum_{i=0}^{n} \partial q/\partial x_i(P) x_i = 0$. Supposons que $X(k)$ est non vide et fixons un point $P_0 \in X(k)$.
   (a) Montrer que l'ensemble des droites $L \subset \mathbb{P}^n_k$ qui passent par le point P_0 s'identifie à $\mathbb{P}^{n-1}_k$. Montrer que l'ensemble des droites qui en plus ne sont pas tangentes à X forme un ouvert $U_{P_0} \subset \mathbb{P}^{n-1}_k$.
   (b) Montrer qu'une droite $L \in U_{P_0}$ coupe X en exactement deux points distincts : P_0 et P_L.
   (c) En déduire que la projection $U \to X$, $L \mapsto P_L$ est bijective sur son image.
3. (**La cubique gauche**) Soit k un corps infini, soit $\Phi : \mathbb{P}^1_k \to \mathbb{P}^3_k$ le morphisme

$$\Phi(x,y) = (x^3, x^2y, xy^2, y^3)$$

   et soit X l'image de Φ.
   (a) Montrer que $X = V(I)$ où $I = (XT - YZ, Y^2 - XZ, Z^2 - YT)$ dans les coordonnées homogènes $(X : Y : Z : T)$ de $\mathbb{P}^3_k$.
   (b) Montrer que $I(X) = I$ (on peut commencer par montrer que tout $f \in k[X,Y,X,T]$ homogène s'écrit modulo I comme $f = a(X,T) + b(X,T)Y + c(X,T)Z$).

(c) Montrer que I ne peut pas être engendré par deux générateurs.

(d) Montrer que X peut s'écrire comme $X = V(Z^2 - YT, P)$ où P est un polynôme homogène de degré trois qu'on précisera.

(Correction :

(a) On vérifie immédiatement que si $x \in X$, alors $x \in V(I)$. Inversement, soit $x = (X : Y : Z : T) \in V(I)$. Si $X \neq 0$, on trouve $Z/X = (Y/X)^2$ et $T/X = (Y/X)(Z/X) = (Y/X)^3$, d'où $x \in X$. On vérifie de même le cas $T \neq 0$. Enfin, les conditions $X = T = 0$ impliquent $Y = Z = 0$, ce qui n'est pas possible.

(b) Soit $f \in k[X, Y, Z, T]$ un polynôme homogène. Notons que, modulo I, on peut écrire f sous la forme

$$f = a(X, T) + b(X, T)Y + c(X, T)Z$$

(pour le voir, modulo I on peut remplacer d'abord YZ par XT dans tous les monômes qui contiennet YZ, de sorte qu'aucun monôme contient Y et Z au même temps. Ensuite on remplace Y^{2m} par $(XZ)^m$ et Y^{2m+1} par $X^m Z^m Y = X^{m+1} Z^{m-1} T$, et de même pour les puissances de Z. Après ces deux opérations on a encore qu'aucun monôme contient Y et Z au même temps et le dégré en Y et en Z a diminué. On continue jusqu'à ce que l'on n'obtient que des facteurs linéaires.) Si f s'annule en tout point de X, on a donc $a(u^3, v^3) + b(u^3, v^3)u^2 v + c(u^3, v^3)uv^2$ pour tous $u, v \in k$. Puisque k est infini, cela implique que tous les coefficients des polynômes $a, b.c$ sont nuls, d'où $f \in I$.

(c) Supposons le contraire. Supposons $I = (f, g)$ Comme I ne contient pas de polynômes avec des termes linéaires non nuls, on a de même pour f et g. Écrivons

$$f = f_2 + f' \text{ et } g = g_2 + g',$$

où f_2, g_2 sont homogènes de degré 2, et f', g' sont de degré plus grand. On peut donc exprimer $XT - YZ$, $Y^2 - XZ$ et $Z^2 - YT$ comme des combinaisons linéaires de f_2 et g_2 ; ils sont donc linéairement dépendants. Contradiction.

(d) On vérifie que

$$F = X(XT - YZ) + Y(Y^2 - XZ) = Y^3 - 2XYZ + X^2 T$$

convient. Soit $J = V(Z^2 - YT, F)$. Si $(X : Y : Z : T) \in V(J)$, on a : si $T = 0$ on obtient $Z = 0$ et $Y = 0$ et on obtient bien un point de X ; si $T \neq 0$ on a $Y/T = (Z/T)^2$ et $(X/T - (Z/T)^2)^2 = 0$, dóu $X/T = (Z/T)^3$ et on obtient bien un point de X. On en déduit que $V(J) = X$.)

4. (**Plongement de Segre**) Montrer que l'application $\mathbb{P}_k^n \times \mathbb{P}_k^m \to \mathbb{P}_k^{mn+m+n}$ définie par

$$((x_0 : \ldots : x_n), (y_0 : \ldots y_m)) \mapsto (x_i y_j)_{0 \leq i \leq n, 0 \leq j \leq m}$$

donne une bijection entre $\mathbb{P}_k^n \times \mathbb{P}_k^m$ et une sous-variété algébrique fermée de $\mathbb{P}_k^n \times \mathbb{P}_k^m$.

5. Montrer que la cubique

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

est lisse si et seulement si $4A^3 + 27B^2 \neq 0$.

6. Soit k un corps algébriquement clos et soit E une courbe elliptique sur k définie par l'équation $y^2 = x^3 + ax + b$. Écrivons $f(x) = x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3)$. Montrer que le déterminant $\Delta = -(4a^3 + 27b^2)$ de E s'écrit comme

$$\Delta = [(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)]^2.$$

7. Soit k un corps algébriquement clos.
   (a) Soit E une courbe elliptique sur k donnée par l'équation $y^2 = x^3+Ax+B$. Montrer que $(x, y) \to (x, -y)$ est un homomorphisme (de groupes) de E dans lui-même.
   (b) Soit E une courbe elliptique sur k donnée par l'équation $y^2 = x^3 + B$. Montrer que $(x, y) \to (\zeta x, -y)$, où $\zeta^3 = 1$ une racine primitive de l'unité, est un endomorphisme de E.
   (c) Soit E une courbe elliptique sur k donnée par l'équation $y^2 = x^3 + Ax$. Montrer que $(x, y) \to (-x, iy)$ est un endomorphisme de E dans lui-même.

8. **[j-invariant]** Soit k un corps algébriquement clos de caractéristique différente de 2 ou 3. Soit E une courbe elliptique donnée par une équation $y^2 = x^3 + Ax + B$. Définissons le j-invariant de E par la formule

$$j = j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

   (a) Soient E_i deux courbes elliptiques données par des équations $y^2 = x^3 + A_ix + B_i$. Montrer que si $j(E_1) = j(E_2)$, alors il existe $\mu \in K$, $\mu \neq 0$ tel que $A_2 = \mu^4 A_1$ et $B_2 = \mu^6 B_1$.
   (b) En déduire que l'application $x_2 = \mu^2 x_1$, $y_2 = \mu^3 y_1$ induit un isomorphisme (de groupes) entre E_1 et E_2.

9. (a) Soit E une courbe elliptique sur un corps k (de caractéristique différente de 2) définie par l'équation $y^2 = (x-e_1)(x-e_2)(x-e_3)$. Determiner tous les points d'ordre 2 de E. En déduire la structure du groupe $E[2] = \{P \in E(k), 2P = 0\}$.
   (b) Soit $a \in \mathbb{Z}$ un entier qui n'est divisible par aucune puissance quatrième (sauf 1) et soit E une courbe elliptique $y^2 = x^3 + ax$. On se propose de trouver tous les points d'ordre 2^n de $E(\mathbb{Q})$.
      i. Déterminer tous les points d'ordre 2.

ii. Soient $(x, y), (u, v) \in E$ avec $(x, y) = 2(u, v)$. Montrer que $x = (u^2 - a)^2/4v^2$.

iii. Soit P un point d'ordre 2. Montrer que $P = 2Q$ implique $a = 4$. Trouver les points d'ordre 4.

iv. Conclure.

10. Soit E une courbe elliptique sur un corps algébriquement clos k (de caractéristique différente de 3). Montrer que le sous-groupe $E[3] = \{P, 3P = 0\}$ de E est isomorphe au groupe $\mathbb{Z}/3 \oplus \mathbb{Z}/3$.

Chapitre 3

Courbes elliptiques sur les corps finis

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de cardinal $q = p^n$ avec p premier. Le théorème célèbre de Hasse permet d'estimer le nombre (fini) des points $E(\mathbb{F}_q)$:

Théorème 3.0.1. [Hasse] *Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de cardinal q. Alors*

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

On sait aussi [1] que pour tout entier a premier à p et tel que $|a| < 2\sqrt{q}$ il existe une courbe elliptique E sur $\mathbb{F}_q$ avec $\#E(\mathbb{F}_q) = q + 1 - a$.

On commence par une approche qui vient de la théorie analytique des nombres qui permet de donner une preuve relativement élémentaire de ce théorème dans deux cas particuliers : $q = p$ et E donnée par $y^2 = x^3 + D$ ou $y^2 = x^3 - Dx$, où D est un entier non nul.

3.1 Caractères, sommes de Gauss et Jacobi.

Définition 3.1.1. Un **caractère multiplicatif** sur $\mathbb{F}_p$ est une application $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$ telle que $\chi(ab) = \chi(a)\chi(b)$.

Proposition 3.1.2. *Soit χ un caractère multiplicatif et soit $a \in \mathbb{F}_p^*$. Alors*
(i) $\chi(1) = 1$ *;*
(ii) $\chi(a)^{p-1} = 1$*, i.e.* $\chi(a)$ *est une racine* $p-1$*-ième de l'unité ;*
(iii) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Démonstration. (i) On utilise que $\chi(1) = \chi(1) \cdot \chi(1)$ et que $\chi(1) \neq 0$ d'après la définition d'un caractère.
(ii) Pour $a \in \mathbb{F}_p^*$, on a $a^{p-1} = 1$. On a donc $(\chi(a))^{p-1} = \chi(a^{p-1}) = \chi(1) = 1$ d'après (i).

1. ce résultat utilise des méthodes élaborées et ne pourrait pas être présentée dans le contexte de ce cours.

(iii) On a $\chi(a)\chi(\underline{a^{-1}}) = \chi(aa^{-1}) = 1$, d'où $\chi(a^{-1}) = \chi(a)^{-1}$. D'après (ii), $|\chi(a)|^2 = \chi(a)\overline{\chi(a)} = 1$.

□

Exemples :

1. le symbôle de Legendre (a/p) est un caractère ;
2. le caractère trivial : $\epsilon(a) = 1$ pour tout $a \in \mathbb{F}_p^*$.
3. Rappelons que $\mathbb{F}_p^*$ est un groupe cyclique d'ordre $p-1$. Soit g un générateur de ce groupe. Pour définir un caractère multiplicatif sur $\mathbb{F}_p$ il suffit de donner sa valeur en g. On définit un caractère $\lambda : \mathbb{F}_p^* \to \mathbb{C}$ par $\lambda(g) = e^{2\pi i/(p-1)}$ (on a donc $\lambda(g^k) = e^{2\pi ik/(p-1)}$). On a $\lambda^{p-1} = 1 : \lambda(g)^{p-1} = \lambda(g^{p-1}) = \lambda(1) = 1$. De plus, si n est tel que $\lambda^n = 1$ on a $\lambda(g)^n = \lambda(g^n) = e^{2\pi in/(p-1)} = 1$, on a donc nécessairement $p-1 \,|\, n$.
4. On peut étendre un caractère χ sur $\mathbb{F}_p$ en posant : $\chi(0) = 0$ si $\chi \neq \epsilon$ et $\chi(0) = 1$ si $\chi \neq \epsilon$.

L'ensemble des caractères forme un groupe : si χ, λ sont deux caractères, on pose $(\chi\lambda)(a) = \chi(a)\lambda(a)$ et $\chi^{-1}(a) = (\chi(a))^{-1}$.

Proposition 3.1.3. *Le groupe des caractères est un groupe cyclique d'ordre $p-1$. Si $a \in \mathbb{F}_p^*, a \neq 1$, alors il existe un caractère χ tel que $\chi(a) \neq 1$.*

Démonstration. D'après l'exemple 3 ci-dessus, un caractère χ est déterminé par sa valeur $\chi(g)$ et d'après la proposition 3.1.2, $\chi(g)$ est une racine $(p-1)$-ième de l'unité. On a donc qu'on a au plus $p-1$ caractères. Toujours d'après l'exemple 3, les caractères $\epsilon, \lambda, \lambda^2, \ldots, \lambda^{p-1}$ sont tous distincts, ce sont donc exactement les $p-1$ caractères sur $\mathbb{F}_p$ et le groupe des caractères est cyclique. Si $a \in \mathbb{F}_p^*, a \neq 1$, alors $\lambda(a) \neq 1$. □

Proposition 3.1.4. *(i) pour $\chi \neq \epsilon$ un caractère multiplicatif on a $\sum_{a\in\mathbb{F}_p} \chi(a) = 0$;*
(ii) pour $a \in \mathbb{F}_p^*, a \neq 1$ on a $\sum_\chi \chi(a) = 0$.

Démonstration. (i) Comme $\chi \neq \epsilon$, il existe $b \in \mathbb{F}_p$ tel que $\chi(b) \neq 1$. On vérifie que $\chi(b)\sum_{a\in\mathbb{F}_p} \chi(a) = \sum_{a\in\mathbb{F}_p} \chi(a)$, d'où $\sum_{a\in\mathbb{F}_p} \chi(a) = 0$.
(ii) D'après la proposition précédente il existe un caracère λ tel que $\lambda(a) \neq 1$. On a donc $\lambda(a)\sum_\chi \chi(a) = \sum_\chi \chi(a) = 0$.

□

Les deux énoncés qui suivent expliquent comment on peut utiliser les caractères pour résoudre des équations sur $\mathbb{F}_p$.

Lemme 3.1.5. *Soit $a \in \mathbb{F}_p^*$.*

1. *L'équation $x^n = a$ admet une solution si et seulement si $a^{p-1/d} = 1$ où $d = (n, p-1)$.*
2. *Supposons que $n \mid p-1$. Si l'équation $x^n = a$ n'admet pas de solution, alors il existe un caractère χ tel que $\chi(a) \neq 1$ et $\chi^n = \epsilon$.*

Démonstration. 1. Résulte du fait que le groupe $\mathbb{F}_p^*$ est cyclique d'ordre $(p-1)$.

2. Soient g et λ comme dans l'exemple 3 ci-dessus. Soit $n' = p - 1/n$. Soit $\chi = \lambda^{n'}$. On a donc $\chi^n = \epsilon$. Écrivons $a = g^s$, on a que n ne divise pas s d'après la condition que l'équation $x^n = a$ n'admet pas de solution. On en déduit $\chi(a) = \chi(g)^s = e^{2\pi i(s/n)} \neq 1$.

□

Proposition 3.1.6. *Soit $a \in \mathbb{F}_p^*$. Soit n un entier tel que $n|p-1$. Soit $N(x^n = a)$ le nombre des solutions dans $\mathbb{F}_p^*$ de l'équation $x^n = a$. On a*

$$N(x^n = a) = \sum_{\chi, \chi^n = \epsilon} \chi(a).$$

Démonstration. 1. Si $a = 0$ alors $N(x^n = a) = 1$ et $\sum_{\chi,\chi^n=\epsilon} \chi(0) = 1$ car pour tout caractère $\chi \neq \epsilon, \chi(0) = 0$.

2. Supposons que l'équation $x^n = a$ admet une solution : $a = b^n$. Notons que, puisque le groupe des caractères est cyclique, on a exatement n caractères tels que $\chi^n = \epsilon$. Pour un tel caractère χ on a $\chi(a) = \chi(b^n) = \chi(b)^n = \chi^n(b) = \epsilon(b) = 1$. On a donc $\sum_{\chi,\chi^n=\epsilon} \chi(a) = n = N(x^n = a)$.
3. Supposons que l'équation $x^n = a$ n'admet pas de solution. Soit χ comme dans la partie 2 de la proposition ci-dessus. On a $\chi(a) \sum_{\chi',\chi'^n=\epsilon} \chi'(a) = \sum_{\chi',\chi'^n=\epsilon} \chi'(a)$, d'où $\sum_{\chi',\chi'^n=\epsilon} \chi'(a) = 0$ car $\chi(a) \neq 1$.

□

Définition 3.1.7. Soit χ un caractère de $\mathbb{F}_p$ et soit $a \in \mathbb{F}_p$. Soit $\zeta = e^{2\pi i/p}$. On définit

$$g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t)\zeta^{at}$$

la somme de Gauss du caractère χ. On définit $g(\chi) = g_1(\chi)$.

Lemme 3.1.8. $g_a(\chi) = \begin{cases} \chi(a^{-1})g_1(\chi) & a \neq 0, \chi \neq \epsilon \\ 0 & a \neq 0, \chi = \epsilon \\ 0 & a = 0, \chi \neq \epsilon \\ p & a = 0, \chi = \epsilon. \end{cases}$

Démonstration. 1. Supposons $a \neq 0, \chi \neq \epsilon$. Alors $\chi(a)g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(at)\zeta^{at} = g_1\chi$.

2. Supposons $a \neq 0, \chi = \epsilon$. Alors $g_a(\chi) = \sum_{t\in\mathbb{F}_p} \zeta^{at} = \frac{1-\zeta^{ap}}{1-\zeta^a} = 0$.
3. Supposons $a = 0, \chi \neq \epsilon$. Alors $g_a(\chi) = \sum_{t\in\mathbb{F}_p} \chi(t) = 0$ par la proposition 3.1.4.
4. Supposons $a = 0, \chi = \epsilon$. Alors $g_a(\chi) = \sum_{t\in\mathbb{F}_p} 1 = p$.

□

Proposition 3.1.9. *Si $\chi \neq \epsilon$, $|g(\chi)| = \sqrt{p}$.*

Démonstration. On pose $S(\chi) = \sum_a g_a(\chi)\overline{g_a(\chi)}$. Par le lemme ci-dessus, pour $a \neq 0$ on a

$$g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})\chi(a)g(\chi)\overline{g(\chi)} = |g(\chi)|^2.$$

Comme $g_0(\chi) = 0$ par le lemme ci-dessus, on a $S(\chi) = (p-1)|g(\chi)|^2$. Par ailleurs,

$$S(\chi) = \sum_a (\sum_u \sum_v \chi(u)\overline{\chi(v)})\zeta^{a(u-v)}.$$

Or $\sum_t \zeta^{ct} = p$ si $c = 0$ et $\sum_t \zeta^{ct} = \frac{1-\zeta^{cp}}{1-\zeta^c} = 0$ si $c \neq 0$. On obtient

$$S(\chi) = \sum_u \sum_v \chi(u)\overline{\chi(v)}\delta(u,v)p = (p-1)p.$$

On a donc $(p-1)|g(\chi)|^2 = (p-1)p$, d'où le résultat.

□

Définition 3.1.10. Soient χ et λ des caractères de $\mathbb{F}_p$. La somme de Jacobi $J(\chi,\lambda)$ est définie par $J(\chi,\lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$.

Proposition 3.1.11. *Soient χ et λ des caractères de $\mathbb{F}_p$.*
(i) $J(\epsilon,\epsilon) = p$;
(ii) pour $\chi \neq \epsilon$, on a $J(\epsilon,\chi) = 0$;
(iii) pour $\chi \neq \epsilon$, on a $J(\chi,\chi^{-1}) = -\chi(-1)$;
(iv) si $\chi\lambda \neq \epsilon$ alors $J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$;
(v) si $\chi\lambda \neq \epsilon$ alors $|J(\chi,\lambda)| = \sqrt{p}$.

Démonstration. L'assertion (i) est immédiate, l'assertion (ii) résulte de la proposition 3.1.4, l'assertion (v) résulte de (iv). Montrons (iii). On a

$$J(\chi,\chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{a+b=1,b\neq 0} \chi(a/b) = \sum_{a\neq 1} \chi(a/1-a) = [c = 1/1-a] = \sum_{c\neq -1} \chi(c) = [\text{par } 3.1.4] = -\chi(-1).$$

Montrons (iv). On a

$$g(\chi)g(\lambda) = (\sum_a \chi(a)\zeta^a)(\sum_b \lambda(b)\zeta^b) =$$
$$= \sum_{a,b} \chi(a)\lambda(b)\zeta^{a+b} = \sum_t (\sum_{a+b=t} \chi(a)\lambda(b))\zeta^t.$$

Si $t = 0$, on a $\sum_a \chi(a)\lambda(-a) = \lambda(-1)\sum_a (\chi\lambda)(a) = 0$ par la proposition 3.1.4. Si $t \neq 0$, on a $\sum_{a+b=t} \chi(a)\lambda(b) = \sum_{a'+b'=1} \chi(a't)\lambda(b't) = (\chi\lambda(t))J(\chi,\lambda)$. On a donc $g(\chi)g(\lambda) = \sum_t (\chi\lambda(t))\zeta^t J(\chi,\lambda) = J(\chi,\lambda)g(\chi\lambda)$. □

3.2 Théorème de Hasse : cas particuliers.

3.2.1 Cas $E : y^2 = x^3 + D$

Soit $p \geq 5$ un premier et soit E une courbe elliptique définie sur $\mathbb{F}_p$ par l'équation homogène $y^2z = x^3 + Dz^3$, $D \neq 0$. Soit N_p l'ensemble des points $E(\mathbb{F}_p)$. Comme E a un point à l'infini, on a

$$N_p = 1 + N(y^2 = x^3 + D).$$

On a deux cas à considérer :

1. Supposons $p \equiv 2(mod\ 3)$. Alors $(p-1, 3) = 1$ et l'application $x \mapsto x^3$ est un automorphisme de $\mathbb{F}_p^*$. Pour $a = y^2$ fixé, l'équation $x^3 = a^2 - D$ admet une unique solution. Ainsi $N(y^2 = x^3 + D) = p$ et $N_p = 1 + p$.
2. $p \equiv 1(mod\ 3)$. Soit χ un caractère multiplicatif d'ordre 3 et ρ un caractère multiplicatif d'ordre 2 sur $\mathbb{F}_p^*$. On a

$$N(y^2 = x^3 + D) = \sum_{a+b=D} N(y^2 = a)N(x^3 = -b) = [\text{par } 3.1.6]$$
$$= \sum_{a+b=D} (1 + \rho(a))(1 + \chi(-b) + \chi^2(-b)) =$$
$$= p + \sum_{a+b=D} \rho(a)\chi(b) + \sum_{a+b=D} \rho(a)\chi^2(b) = [a = Da', b = Db']$$
$$= p + \rho\chi(D)J(\rho,\chi) + \overline{\rho\chi(D)J(\rho,\chi)}.$$

Puisque $|J(\rho,\chi)| = \sqrt{p}$ d'après la proposition 3.1.11, on déduit $|N_p - 1 - p| < 2\sqrt{p}$. □

3.2.2 Cas $E : y^2 = x^3 - Dx$

Soit E une courbe elliptique sur $\mathbb{F}_p$, $p \geq 2$, définie par l'équation homogène $y^2z = x^3 - Dxz^2$, avec $D \neq 0$. Soit N_p l'ensemble des points $E(\mathbb{F}_p)$. Comme dans le cas précédent, on a

$$N_p = 1 + N(y^2 = x^3 - Dx).$$

Lemme 3.2.1. *Soit C la courbe affine $y^2 = x^3 - Dx$ et soit C' la courbe affine $u^2 = v^4 + 4D$. Soit*

$$T : \mathbb{A}^2 \to \mathbb{A}^2$$
$$u, v \mapsto \frac{u + v^2}{2}, \frac{v(u + v^2)}{2}$$

et soit

$$S : \mathbb{A}^2 \to \mathbb{A}^2$$
$$x, y \mapsto 2x - \frac{y^2}{x^2}, \frac{y}{x}.$$

Alors T envoie C' dans C et S enoie $C \setminus \{0, 0\}$ dans C'. De plus, la restriction $T \circ S | C \setminus \{0, 0\}$ est l'identité sur C' et la restriction de $S \circ T$ à C' est l'identité sur C.

Démonstration. Vérification immédiate d'après les définitions des applications T et S. □

Soit $N' = N(u^2 = v^4 + 4D)$. D'après le lemme ci-dessus, $N_p = 2 + N'$. On a deux cas à considérer :

1. Supposons $p \equiv 3 (mod\ 4)$. Alors -1 n'est pas un carré, i.e. tout élément $a \in \mathbb{F}_p$ s'écrit comme $a = \pm b^2$. En particulier, $a^2 = b^4$, i.e. tout carré est une puissance 4ème. Ainsi $N' = N(y^2 = v^4 + 4D) = N(u^2 = v^2 + 4D) = p - 1$ et $N_p = 2 + N' = 1 + p$.
2. $p \equiv 1 (mod\ 4)$. Soit λ un caractère multiplicatif d'ordre 4 et $\rho = \lambda^2$. On a

$$N(u^2 = v^4 + 4D) = \sum_{a+b=4D} N(u^2 = a)N(v^4 = -b) = [\text{car } J(\rho, \rho) = -1] =$$
$$= p - 1 + \overline{\lambda(-4D)} J(\rho, \lambda) + \lambda(-4D)\overline{J(\rho, \lambda)}.$$

Puisque $|J(\rho, \lambda)| = \sqrt{p}$ d'après la proposition 3.1.11, on déduit $|N_p - 1 - p| < 2\sqrt{p}$. □

3.3 Endomorphismes

Dans cette section k est un corps algébriquement clos.

Définition 3.3.1. Soit E une courbe elliptique définie sur k. On définit un **endomorphisme** de E comme une application $\alpha : E \to E$ donnée par des fonctions rationnelles et qui vérifie

$$\alpha(P + Q) = \alpha(P) + \alpha(Q).$$

Si E est donnée par l'équation affine (2.2), on peut donc écrire

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)).$$

Dans ce qui suit, on va exprimer α de façon plus simple et en particulier définir α dans les points où le dénominateur de R_1 ou de R_2 s'annule (en coordonnées projectives.)

Puisque $(x,y) \in E$, on peut supposer que les fractions R_1, R_2 n'ont pas de terme en y^2 et écrire

$$R_i(x) = \frac{p_1^i(x) + p_2^i(x)y}{q_1^i(x) + q_2^i(x)y} = \frac{(p_1^i(x) + p_2^i(x)y)(q_1^i(x) - q_2^i(x)y)}{(q_1^i(x))^2 - (q_2^i(x))^2(x^3 + ax + b)} = \frac{r_1^i(x) + r_2^i(x)y}{q^i(x)}$$

pour certains polynômes r_1^i, r_2^i, q^i.

Ensuite, puisque α est un endomorphisme, on a $\alpha(x,-y) = -\alpha(x,y)$ d'où $R_1(x,-y) = R_1(x,y)$ et $R_2(x,-y) = -R_2(x,y)$. On en déduit que l'on peut écrire

$$\alpha(x,y) = (\frac{p(x)}{q(x)}, \frac{s(x)y}{t(x)}) \tag{3.1}$$

avec $p, q, r, t \in k[x]$ tels que p, q n'ont pas de racine commune et s, t n'ont pas de racine commune.

Définition 3.3.2. On définit le **degré** de α par

$$deg\alpha = max\{deg\, p(x), deg\, q(x).\}$$

On dit que α est **séparable** si la derivée de la fraction $p(x)/q(x)$ n'est pas identiquement nulle.

On va maintenant définir α aux points où le dénominateur $q(x)$ ou $t(x)$ s'annule. Puisque $\alpha(x,y) \in E$ on a

$$\frac{(x^3 + ax + b)s(x)^2}{t(x)^2} = \frac{p(x)^3 + ap(x)q(x)^2 + bq(x)^3}{q(x)^3}.$$

On a en particulier l'égalité

$$(x^3 + ax + b)s(x)^2 q(x)^3 = (p(x)^3 + ap(x)q(x)^2 + bq(x)^3)t(x)^2$$

en tout point x tel que $q(x)t(x) \neq 0$. Puisque l'ensemble des racines de t et q est un ensemble fini et k est algébriquement clos, l'égalité ci-dessus est vraie pour tout $x \in k$. Écrivons

$$f(x) = x^3 + ax^2 + b = (x - e_1)(x - e_2)(x - e_3).$$

Soit $S \subset \{e_1, e_2, e_3\}$ l'ensemble des racines communes de $t(x)$ et $x^3 + ax + b$. Puisque $t(x)$ et $s(x)$ n'ont pas de racines communes et le polynôme $x^3 + ax + b$ n'a que des racines simples, on déduit que $q(x) = u(x)^2 \prod_S (x - e_i)$ et $t(x) = u(x)^3 \prod_S (x - e_i)^2$.

On peut donc écrire α dans les coordonnées projectives :

$$\alpha(x,y) = (p(x)u(x)\prod_S(x-e_i) : s(x)y : u(x)^3\prod_S(x-e_i)^2). \tag{3.2}$$

Si $q(x) \neq 0$ on a $u(x)^3\prod_S(x-e_i)^2 \neq 0$ d'après ce qui précède et donc $\alpha(x,y)$ est bien défini. Si $q(x) = 0$, on pose $\alpha(x,y) = O_E$. Ceci peut être justifié comme suit. Si $q(x) = 0$, on a $s(x) \neq 0$. Si $y \neq 0$, alors $\alpha(x,y) = O_E$ d'après la formule ci-dessus. Si $y = 0$, on a alors $x = e_i, i \in S$. On utilise alors que $y^2 = \prod(x-e_i)$ pour réécrire

$$\alpha(x,y) = (p(x)u(x)y : s(x)\prod_{i\notin S}(x-e_i) : u(x)^3y\prod_S(x-e_i)),$$

d'où l'on voit encore que $\alpha(x,y) = O_E$.

Les deux énoncés qui suivent sont importants pour les applications :

Proposition 3.3.3. *Soit α un endomorphisme non nul d'une courbe elliptique E. On a alors*

(i) si α est séparable, alors $\deg\alpha$ est égal au cardinal de l'ensemble $ker(\alpha)$;

(ii) si α n'est pas séparable, alors $\deg\alpha > \#ker(\alpha)$;

Démonstration. On écrit α dans la forme (3.1). Soient $r_1(x) = \frac{p(x)}{q(x)}$, $r_2(x) = \frac{s(x)}{t(x)}$.

(i) Si α est séparable, la fonction $r_1'(x)$ n'est pas identiquement nulle, en particulier $p'q - pq'$ n'est pas un polynôme nul. Soit

$$S = \{x \in k, (p'q - pq')q(x) = 0.\}$$

On a que S est un ensemble fini. On observe que la fonction $r_1(x)$ prend une infinité de valeurs, en particulier, il existe $P = (c,d) \in E(k)$ un point distinct de O_E tel que

1. $c \neq 0, d \neq 0, c \notin r_1(S), (c,d) \in \alpha(E(k))$

2. $deg\,(p(x) - cq(x)) = deg\,(\alpha)$.

Soit

$$S' = \{(x_0,y_0) \in E(k) \,|\, \alpha(x_0,y_0) = (c,d).\}$$

On va montrer que l'ensemble S' contient exactement $deg(\alpha)$ éléments. En effet, si $(x_0,y_0) \in S'$, on a $\frac{p(x_0)}{q(x_0)} = c$ et $y_0r_2(x_0) = d$. Puisque $(c,d) \neq O_E$ et $d \neq 0$, on a que $r_2(x_0) \neq 0$ est bien défini et $y_0 = \frac{d}{r_2(x_0)}$. On a donc que le cardinal de S' est le nombre d'éléments $x_0 \in k$ tels que $p(x_0) = cq(x_0)$ Puisque $deg\,(p(x) - cq(x)) = deg\,(\alpha)$, il suffit de montrer que le polynôme $p(x) - cq(x)$ n'a que des racines simples. Sinon, il existe $x_1 \in k$ tel que $p(x_1) = cq(x_1)$, $p'(x_1) = cq'(x_1)$, donc x_1 est une racine du polynôme $p'q - pq'$ (car $c \neq 0$), d'où $c \in r_1(S)$, contradiction avec le choix de c. On a donc que $\#S' = \#ker(\alpha) = deg\,\alpha$.

(ii) Ce cas est analogue à (i) avec la différence que le polynôme $p(x) - cq(x)$ a des racines multiples et donc $\#ker(\alpha) < deg\,\alpha$.

□

Proposition 3.3.4. *Soit α un endomorphisme non nul d'une courbe elliptique E. Alors $\alpha : E \to E$ est une application surjective.*

Démonstration. Le point $P = O_E$ est l'image de O_E. Soit $P = (c, d)$ un point de E différent de O_E. On cherche (x, y) tels que $\alpha(x, y) = (c, d)$. On écrit α dans la forme (3.1). Soit $h(x) = p(x) - cq(x)$. On a deux cas :

1. Si $h(x)$ n'est pas un polynôme constant, soit x_0 une racine de h. Si $q(x_0) = 0$, alors $p(x_0) = 0$ et on obtient une contradiction avec le fait que p et q n'ont pas de racines communes. On a donc $q(x_0) \neq 0$. Soit y_0 une des racines de $x_0^3 + ax_0 + b$. D'après (3.2), on a $\alpha(x_0, y_0) = (c, d')$ pour $d' \in k$. Comme (c, d') est un point de E, on a $d = \pm d'$ et donc $(c, d) = \alpha(x_0, \pm y_0)$.
2. Supposons que $h(x)$ est un polynôme constant. La fraction $\frac{p(x)}{q(x)}$ n'est pas constante (en effet, $ker(\alpha)$ est fini d'après la proposition précédente, $E(k)$ est infini, on a donc un nombre fini de points dont l'image par α est un point fixé). On a donc au plus un élément $c \in k$ tel que $p(x) - cq(x)$ est un polynôme constant. D'après le cas précédent, on a donc au plus deux points (c, d) et $(c, -d)$ qui ne sont pas dans l'image de α (avec $d^2 = c^3 + ac + b$). Soit $(c_1, d_1) \in E(k)$ tel que $(c_1, d_1) + (c, d) \neq (c, \pm d')$. On a donc que (c_1, d_1) et $(c_1, d_1) + (c, d)$ sont dans l'image de α, et donc (c, d) l'est aussi puisque α est un endomorphisme.

□

Notons qu'étant donné un endomorphisme $\alpha : E \to E$, cela peut être assez technique de determiner le degré de α, ainsi que si α est séparable. Si $\alpha, \beta : E \to E$ sont deux endomorphismes, alors on définit leurs somme par la formule $(\alpha + \beta)(P) = \alpha(P) + \beta(P)$. Comme l'addition des points sur une courbe elliptique est donnée par des fractions rationnelles, on voit que $\alpha + \beta$ est bien un endomorphisme de E. De façon analogue, on définit une combinaison linéaire d'endomorphismes. On dispose aussi d'une formule pour determiner son degré (voir les exercices pour la preuve) :

Proposition 3.3.5. *Soient α, β deux endomorphismes non nuls d'une courbe elliptique E. Soient r, s deux entiers. Alors*

$$deg\, r\alpha + s\beta = r^2 deg\,\alpha + s^2 deg\,\beta + rs(deg\,\alpha + \beta - deg\,\alpha - deg\,\beta).$$

Dans les exemples qui suivent, on donne quelques applications, en admettant des résultats sur la séparabilité et le degré.

3.3.1 Endomorphisme de Frobenius et théorème de Hasse

Soit k une clôture algébrique du corps fini $\mathbb{F}_q$ à $q = p^n$ éléments. **Le morphisme de Frobenius** ϕ_q sur k est l'application $x \mapsto x^q$. Pour $x, y \in k$ on a $(x+y)^q = x^q + y^q$, donc ϕ_q est bien un homomorphisme (de groupes additifs). De plus, par construction, le corps $\mathbb{F}_q$ est le corps de décomposition du polynôme $x^q - x$, d'où

$$x \in \mathbb{F}_q \Leftrightarrow \phi_q(x) = x. \tag{3.3}$$

Soit $E : y^2 = x^3 + ax + b$ une courbe ellitique définie sur $\mathbb{F}_q$. Comme $a^q = a$ et $b^q = b$, on a pour tout $P = (x, y) \in E(k)$,

$$y^{2q} = (x^3 + ax + b)^q = x^{3q} + ax^q + b, \text{ i.e. } (x^q, y^q) \in E(k).$$

En utilisant les formules de la loi explicite (Proposition 2.2.5), on montre de même que ϕ_q induit un endomorphisme de E

$$\phi_q(x, y) = (x^q, y^q)$$

qu'on appelle aussi **endomorphisme de Frobenius**. La condition (3.3) donne

$$P \in E(\mathbb{F}_q) \Leftrightarrow \phi_q(P) = P.$$

On voit donc que

$$E(\mathbb{F}_q) = ker(\phi_q - 1). \tag{3.4}$$

D'après la définition, on voit que l'endormorphisme de Frobenius ϕ_q n'est pas séparable et que $deg\, \phi_q = q$. Plus généralement, soient r, s des entiers non nuls. On peut montrer que l'endomorphisme $r\phi_q - s$ est séparable si et seulement si p ne divise pas s.

Avec les résultats sur les endomorphismes ci-dessus, on peut maintenant donner la preuve du théorème de Hasse.

Démonstration du théorème 3.0.1.

On a $E(\mathbb{F}_q) = ker(\phi_q - 1)$ d'après (3.4). Comme le morphisme $\phi_q - 1$ est séparable, la proposition 3.3.3 donne $deg(\phi_q - 1) = \#ker(\phi_q - 1)$ Soit

$$a_q = q + 1 - \#E(\mathbb{F}_q) = q + 1 - deg(\phi_q - 1).$$

Soient r, s deux entiers avec $(s, q) = 1$. On a donc que l'endomorphisme $r\phi_q - s$ est séparable de degré (voir proposition 3.3.5)

$$deg\, r\phi_q - s = r^2 q + s^2 + rs(deg\,(\phi_q - 1) - q - 1) = r^2 q + s^2 + rsa_q.$$

Puisque $deg\, r\phi_q - s \geq 0$ pour tous r, s, on a

$$q(\frac{r}{s})^2 - a_q \frac{r}{s} + 1 \geq 0.$$

Or les rationnels $\frac{r}{s}$ avec $(s,q)=1$ sont denses dans $\mathbb{R}$. On a donc $qx^2 - a_q x + 1 \geq 0$ pour tout $x \in \mathbb{R}$. On obtient donc pour le discriminant :

$$a_q^2 - 4q \leq 0,$$

d'où $|a_q| \leq 2\sqrt{q}$, ce qui termine la preuve du théorème de Hasse. □

Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique sur $\mathbb{F}_q$. Les propriétés du morphisme de Frobenius permettent d'estimer le nombre de points dans $E(\mathbb{F}_{q^n})$ pour toute extension de $\mathbb{F}_q$. On a le résultat suivant (pour la preuve voir l'exercice 6) :

Théorème 3.3.6. *Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ et soit $a_q = q + 1 - \#E(\mathbb{F}_q)$.*

1. *On a $\phi_q^2 - a_q \phi_q + q = 0$.*

2. *Soient α, β les racines du polynôme $x^2 - a_q x + q$. Alors α, β sont des nombres complexes conjugués de valeur absolue $\sqrt{q}$. Pour tout $n > 0$ on a*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

3. *La fonction zêta de la courbe E*

$$Z(E/\mathbb{F}_q, T) = exp(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n}).$$

est la fonction rationnelle $\frac{1 - a_q T + qT^2}{(1-T)(1-qT)}$.

Soit X une variété projective, définie sur un corps fini $\mathbb{F}_q$. On a une notion de lissité, qui généralise celle pour les courbes planes. On dispose aussi de la notion de dimension (pour les coubes planes, la dimension vaut 1.) Supposons que X est lisse, de dimension n. On définit la fonction zêta de X par

$$Z(X/\mathbb{F}_q, T) = exp(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n}) \frac{T^n}{n}).$$

Les **conjectures de Weil** affirment que cette fonction est une fonction rationnelle : $Z(X/\mathbb{F}_q, T) \in \mathbb{Q}(T)$ qui vérifie :

1. (équation fonctionnelle) $Z(X/\mathbb{F}_q, 1/q^N T) = \pm q^{N\epsilon/2} T^\epsilon Z(X/\mathbb{F}_q, T)$ pour certain entier ϵ ;
2. (hypothèse de Riemann) $Z(X/\mathbb{F}_q, T) = \frac{P_1(T) \ldots P_{2N-1}(T)}{P_0(T) P_2(T) \ldots P_{2N}(T)}$ avec $P_0(T) = 1 - T, P_{2N}(T) = 1 - q^N T$ et $P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} T)$, $0 < i < 2N$, avec $|\alpha_{ij}| = q^{1/2}$.

Ces conjectures ont été démontrées en toute généralité par Deligne dans les années 1970.

3.3.2 Points de torsion

Soit E une courbe elliptique sur k (on suppose toujours que le corps k est algébriquement clos). Soit $n \geq 2$ un entier. La multiplication par n donne un endomorphisme $\cdot n : E \to E$. De la même manière que pour la multiplication par 2, on peut donner des formules récursives explicites qui expriment $nP = (x_{nP}, y_{nP})$ en termes de $P = (x_P, y_P)$. Plus précisément, on a l'énoncé suivant (voir l'exercice 8) :

Proposition 3.3.7. *(i) Il existe des polynômes ϕ_n, ψ_n, ω_n avec $(\phi_n, \psi_n) = 1$ tels que*

$$nP = (\frac{\phi_n(x)}{\psi_n(x)^2}, \frac{\omega_n(x,y)}{\psi_n(x)^3}).$$

(ii) Le terme de degré supérieur de $\phi_n(x)$ est x^{n^2}, le terme de degré supérieur de $\psi_n(x)$ est $n^2 x^{n^2-1}$.
(iii) On a $nP = O_E \Leftrightarrow \psi_n(x) = 0$.

On voit alors que le degré de l'endomorpsime de multiplication par n sur E est n^2 et que c'est un morphisme séparable si et seulement si n est premier à la caractéristique de k. On définit **le groupe des points de n-torsion de E** :

$$E[n] = \{P \in E, nP = O_E\}.$$

Il est remarquable que l'on peut determiner la structure de ce groupe pour toute courbe elliptique, indépendamment du corps k :

Théorème 3.3.8. *(i) Si $(n, car.k) = 1$, alors $E[n] = \mathbb{Z}/n \oplus \mathbb{Z}/n$.*
(ii) Si $p = car.k \mid n$, alors $E[n] = \mathbb{Z}/n' \oplus \mathbb{Z}/n'$ ou $E[n] = \mathbb{Z}/n \oplus \mathbb{Z}/n'$, où $n = p^r n'$ et $(n', p) = 1$.

Démonstration. (i) D'après les propriétés ci-dessus et la proposition 3.3.3, $E[n] = deg\,(\cdot n) = n^2$. Le groupe $E[n]$ est un groupe abélien fini d'ordre n^2. D'après le théorème de structure, on a donc

$$E[n] = \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2 \oplus \ldots \oplus \mathbb{Z}/n_s$$

avec $n_i | n_{i+1}, 1 \leq i \leq s-1$. Soit l un premier qui divise n_1. On a donc l^s divise l'ordre de $E[n]$. Or $\#E[l] = l^2$. On obtient $s = 2$ et

$$E[n] = \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2, n_1 | n_2.$$

Par ailleurs, ce groupe est annulé par n, d'où $n_2 | n$. Comme $\#E[n] = n^2 = n_1 n_2$, on déduit que $n_1 = n_2 = n$.

(ii) On va d'abord determiner la structure du groupe $E[p^s]$ pour tout $s > 0$. Comme le morphisme de multiplication par p n'est pas séparable, $\#E[p] < p^2$. Tout élément de $E[p]$ est d'ordre 1 ou p, on a donc $\#E[p]$ est une puissance de p, et donc c'est 1 ou p. Si $\#E[p] = 1$, alors $\#E[p^s] = 1$ pour tout $s > 0$

(on utilise que si $Q \in E[p^s]$, alors $p^{s-1}Q \in E[p]$). Supposons $\#E[p] = p$. Soit $Q \in E[p^s]$. On a donc $pQ \in E[p^{s-1}]$. Par récurrence, $E[p^s]$ est cyclique d'ordre p^s.
Écrivons maintenant $n = p^r n'$. On a alors $E[n] = E[n'] \oplus E[p^r]$. Comme $E[n'] = \mathbb{Z}/n' \oplus \mathbb{Z}/n'$, $E[p^r] = 1$ ou $\mathbb{Z}/p^r$ et $\mathbb{Z}/n' \oplus \mathbb{Z}/p^r \simeq \mathbb{Z}/n'p^r = \mathbb{Z}/n$, on obtient la formule de l'énoncé.

□

De façon analogue, on démontre le théorème de structure pour les points d'une courbe elliptique sur un corps fini (voir les exercices) :

Théorème 3.3.9. *Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$. On a*

$$E(\mathbb{F}_q) = \mathbb{Z}/n \text{ ou } \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2$$

où $n \geq 1$ et $n_1, n_2 \geq 1$ sont des entiers, avec $n_1 \mid n_2$.

L'énoncé suivant donne un outil très important dans l'étude des courbes elliptiques :

Théorème 3.3.10. *Soit k un corps algébriquement clos et soit n un entier premier à la caractéristique de k. Soit E une courbe elliptique sur k. Il existe un accouplement*

$$e_n : E[n] \times E[n] \to \mu_n$$

qu'on appelle **l'accouplement de Weil**, *tel que*

1. *e_n est une application bilinéaire :*

   $$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T),\ e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

   et non-dégénérée :

   $$e_n(S, T) = 1\, \forall T \in E[n] \Rightarrow S = O_E,\ \text{et } e_n(S, T) = 1\, \forall S \in E[n] \Rightarrow T = O_E;$$

2. *$e_n(T, T) = 1$ et $e_n(T, S) = e_n(S, T)^{-1}\ \forall S, T \in E[n]$;*
3. *si $\sigma \in \operatorname{Aut} k$ qui fixe les coefficients a et b de la courbe E, alors $e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$;*
4. *si $\alpha : E \to E$ est un endomorphisme, alors*

   $$e_n(\alpha(S), \alpha(T)) = (e_n(S, T))^{deg\, \alpha}.$$

La preuve de cet énoncé nécessite plus d'outils de la géométrie algébrique et peut être étudié en enseignement d'approfondissement.

Remarques.

1. Si $S = (x, y) \in E(k)$ et si $\sigma \in \operatorname{Aut} k$, le point σS est défini comme $\sigma S = (\sigma x, \sigma y)$.

2. Soit E une courbe elliptique définie sur un corps non-algébriquement clos k et soit $\bar{k}$ une clôture algébrique de k. On note $E[n] = E(\bar{k})[n]$. On a donc l'accouplement de Weil sur $E[n]$. Si maintenant $P, Q \in E(k)$, alors pour tout $\sigma \in \mathrm{Aut}_k\, \bar{k}$ on a $\sigma P = P$ et $\sigma T = T$. D'après la propriété 3 ci-dessus, $e_n(S,T)$ est fixé par tout tel automorphisme σ et en particulier $e_n(S,T) \in k$.

Proposition 3.3.11. *Soit k un corps algébriquement clos, soit n un entier $(n, car.k) = 1$. Soit E une courbe elliptique sur k. Soit $\{T_1, T_2\}$ une base de $E[n] = \mathbb{Z}/n \oplus \mathbb{Z}/n$. Alors $e_n(T_1, T_2)$ est une racine n-ième primitive de l'unité.*

Démonstration. voir exercice 3 ci-dessous. □

Corollaire 3.3.12. *Soit E une courbe elliptique définie sur $\mathbb{Q}$. On écrit $E[n]$ pour le groupe des points de n-torsion de E sur une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$. Alors $E[n] \not\subseteq E(\mathbb{Q})$ si $n \geq 3$.*

Démonstration. Par le théorème 3.3.10.3 et la proposition 3.3.11 ci-dessus, si $E[n] \subseteq E(\mathbb{Q})$, alors $\mu_n \subset \mathbb{Q}$, ce qui n'est pas possible si $n \geq 3$. □

3.3.3 Automorphismes

Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique définie sur un corps algébriquement clos k (on suppose toujours $car(k) \neq 2, 3$). On peut montrer que tout automorphisme θ de E est donné par un changement de variables $x = u^2x', y = u^3y'$ avec $u \in k^*$ et $u^{-4}a = a$ et $u^{-6}b = b$. Rappelons (voir l'exercice 8 de chapitre 2) que le j-invariant de E est défini comme

$$j = j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

On a donc

1. si $j \neq 0, 1728$, le groupe d'automorphismes $Aut(E)$ de E est le groupe fini $\mathbb{Z}/2 = (id, P \mapsto -P)$;
2. si $j = 1728$, $Aut(E) \simeq \mathbb{Z}/4$;
3. si $j = 0$, $Aut(E) \simeq \mathbb{Z}/6$.

3.4 Exercices

1. Soit E une courbe elliptique définie sur un corps algébriquement clos k, $car.k \neq 2, 3$. On écrit $E[2] = \{\infty, P_1, P_2, P_3\}$. Montrer que

$$e_2(P_i, P_j) = -1, i \neq j.$$

2. Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$. Montrer que le groupe $E(\mathbb{F}_q)$ est soit le groupe cyclique $\mathbb{Z}/n$ pour certain $n \geq 1$, soit le groupe $\mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2$ avec $n \geq 1$ et $n_1, n_2 \geq 1$ des entiers, $n_1 \mid n_2$.

3. (a) Soit E une courbe elliptique définie sur un corps algébriquement clos k, $car.k \neq 2, 3$. Rappelons que $E[n] = \mathbb{Z}/n \oplus \mathbb{Z}/n$ pour tout entier n premier à $car\, k$. Soit $\{T_1, T_2\}$ une base de $E[n]$.

   i. Soit $\zeta = e_n(T_1, T_2)$ et soit d un entier tel que $\zeta^d = 1$. Montrer que $e_n(T_1, dT_2) = 1$ et que $e_n(T_2, dT_2) = 1$. En déduire que pour tout $S \in E[n]$ on a $e_n(S, dT_2) = 1$.

   ii. Montrer que $e_n(T_1, T_2)$ est une racine n-ième primitive de l'unité.

   (b) Soit α un endomorphisme de E.

   i. Montrer que α induit un endomorphisme α_n de $E[n]$.

   ii. Soit $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ la matrice de α_n dans la base $\{T_1, T_2\}$. Montrer que

$$deg\, \alpha \equiv det(\alpha_n) (\text{mod } n)$$

   (on pourra exprimer $\zeta^{deg\, \alpha}$ en termes de a, b, c, d.)

   (c) Soient α, β deux endomorphismes de E et r, s deux entiers.

   i. Montrer que

$$det(r\alpha_n + s\beta_n) - r^2 det\alpha_n - s^2 det\beta_n = rs(det(\alpha_n + \beta_n) - det\alpha_n - det\beta_n)$$

   (on peut commencer par montrer que $det(\alpha_n + \beta_n) - det\alpha_n - det\beta_n = Trace(\alpha_n \beta_n^*)$, où β_n^* est la matrice adjointe : si $\beta_n = \left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right)$, alors $\beta_n^* = \left(\begin{smallmatrix} t & -y \\ -z & x \end{smallmatrix}\right)$).

   ii. En déduire que

$$deg\, r\alpha + s\beta = r^2 deg\, \alpha + s^2 deg\, \beta + rs(deg\, (\alpha + \beta) - deg\, \alpha - deg\, \beta).$$

4. Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$. Supposons $E(\mathbb{F}_q) = \mathbb{Z}/n \oplus \mathbb{Z}/n$.

   (a) Montrer que $(n, p) = 1$.

   (b) Montrer que $E(\overline{\mathbb{F}}_q)[n] \subset E(\mathbb{F}_q)$. En déduire que $\mu_n \subset \mathbb{F}_q$.

   (c) Soit $a = q + 1 - \#E(\mathbb{F}_q)$. En déduire que $a \equiv 2 (\text{mod}\, n)$.

   (d) Montrer que $q = n^2 + 1$ ou $q = n^2 \pm n \pm 1$ ou $q = (n \pm 1)^2$.

5. Soit E la courbe elliptique $y^2 = x^3 + x + 1$ sur $\mathbb{F}_5$.

   (a) Montrer que $\#E(\mathbb{F}_5) = 9$.

   (b) Montrer que $3(0, 1) = (2, 1)$ sur E.

   (c) Montrer que $(0, 1)$ engendre le groupe $E(\mathbb{F}_5)$.

6. (a) Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$, $q = p^r$, et soit $a_q = q + 1 - \#E(\mathbb{F}_q)$. Comme dans ce qui précède, on note ϕ_q le morphisme de Frobenius sur E et pour tout entier m premier à q on note $(\phi_q)_m$ l'endomorphisme induit par ϕ_q sur $E(\overline{\mathbb{F}}_q)[m]$. Montrer que

$$det(\phi_q)_m \equiv q \,(\text{mod } m) \text{ et } Trace(\phi_q)_m \equiv a_q \,(\text{mod } m)$$

(On pourra utiliser que $\#Ker(\phi_q - 1) = deg\,(\phi_q - 1) = q + 1 - a_q$, cf. la preuve du théorème de Hasse)

(b) En déduire que l'endomorphisme $\phi_q^2 - a_q\phi_q + q$ est identiquement nul sur $E(\overline{\mathbb{F}}_q)[m]$.

(c) Montrer que le noyau de l'endomorphisme $\phi_q^2 - a_q\phi_q + q$ est infini ; en déduire que le polynôme $g(x) = x^2 - a_q x + q$ annulle ϕ_q.

(d) Supposons que b est un entier tel que le polynôme $x^2 - bx + q$ annulle ϕ_q. En déduire que $(a_q - b)$ annulle $E(\overline{\mathbb{F}}_q)$ et enfn que $a_q = b$.

(e) Soent α, β les racines du polynôme $g(x)$ et soit $g_n(x)$ le polynôme

$$g_n(x) = x^{2n} - (\alpha^n + \beta^n)x^n + q^n.$$

Montrer que $g(x)$ divise $g_n(x)$ pour tout n. En déduire que

$$(\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = 0.$$

(f) En déduire que $E(\mathbb{F}_{q^n})$ est de cardinal $q^n + 1 - (\alpha^n + \beta^n)$.

(g) On définit la fonction zêta de la courbe E par

$$Z(E/\mathbb{F}_q, T) = exp(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n})\frac{T^n}{n}).$$

Montrer que $Z(E/\mathbb{F}_q, T)$ est la fraction rationnelle

$$\frac{1 - a_q T + qT^2}{(1 - T)(1 - qT)}.$$

7. Soit E une courbe elliptique sur $\mathbb{F}_q$ avec $q = p^{2m}$. Supposons que $\#E(\mathbb{F}_q) = q + 1 - 2\sqrt{q}$.

(a) Montrer que $(\phi_q - p^m)^2 = 0$.

(b) En déduire que $\phi_q - p^m = 0$.

(c) Montrer que ϕ_q agit comme l'identité sur $E(\overline{\mathbb{F}}_q)[p^m - 1]$. En déduire que $E(\overline{\mathbb{F}}_q)[p^m - 1] \subset E(\mathbb{F}_q)$.

(d) Montrer que $E(\mathbb{F}_q) = \mathbb{Z}/p^m - 1 \oplus \mathbb{Z}/p^m - 1$.

8. Soit E une courbe elliptique $y^2 = x^3 + ax + b$ définie sur un corps k, $car(k) \neq 2, 3$. On définit les polynômes à division $\psi_m(x, y)$ par récurrence :
$\psi_0 = 0$, $\phi_1 = 1$, $\psi_2 = 2y$
$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$
$\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$
$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$, $m \geq 2$
$\psi_{2m} = [\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)]/2y$, $m \geq 3$.

   (a) Montrer que ψ_n est un polynôme en x, y^2 si n est impair et que $y\psi_n$ est un polynôme en x, y^2, si n est pair.

   (b) On définit $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$
   $\omega_m = [\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2]/4y$. Montrer que ϕ_n est un polynôme en x, y^2, que ω_n est un polynôme en x, y^2 si n est impair, et que $y\omega_n$ est un polynôme en x, y^2 si n est pair.

   (c) D'après la question précédente, on peut définir les polynômes $\phi_n(x)$ et $\psi_n^2(x)$ en remplaçant y^2 par $x^3 + ax + b$ dans les polynômes $\phi_n(x, y)$ et $\psi_n^2(x, y)$. Montrer que $\phi_n(x)$ s'écrit comme la somme de x^{n^2} et de termes de degré inférieur et que $\psi_n(x)^2$ s'écrit comme la somme de $n^2x^{n^2-1}$ et de termes de degré inférieur.

   (d) Montrer que pour $P = (x, y)$ un point de E, on a

$$nP = \left(\frac{\phi_n(x)}{\psi_n(x)^2}, \frac{\omega_n(x, y)}{\psi_n(x)^3}\right)$$

   (e) Montrer que les polynômes $\phi_n(x)$ et $\psi_n(x)^2$ sont premiers entre eux. En déduire que l'endomorphisme de multiplication par n est de degré n^2.

Chapitre 4

Algorithmes qui utilisent les courbes elliptiques

4.1 Factorisation

Pour N un entier on s'intéresse à trouver des algorithmes pour determiner les facteurs premiers de N. La sécurité des cryptosystèmes modernes dépend en particulier du fait que ce problème est très difficile à résoudre en pratique. Dans cette partie on présente une approche qui utilise les courbes elliptiques : l'algorithme **ECM** ("Elliptic Curve Method"), introduit par H. Lenstra dans les années 1980 et développé par R. Brent, P. Montgomery et autres. Cet algorithme est à nos jours le plus efficace en termes de la taille des facteurs de N trouvés (et non pas de N) : il marche en temps $exp(c\sqrt{log\, p(loglog\, p)})$, où p est le plus petit facteur de N. Un des derniers facteurs trouvés est de 74 chiffres : c'est le facteur suivant de $12^{284}+1$ trouvé le 26 octobre 2014 par B. Dodson :

$$26721194531973848954767772351114152203083577206813943149484875628623309473$$

4.1.1 Algorithme $p-1$ de Pollard

Pour commencer, on rappelle l'algorihme $(p-1)$ de Pollard, dont les idées sont aussi utilisées dans l'algorithme ECM. Supposons que N possède un facteur premier p tel que

$$p-1 = q_1^{e_1} q_2^{e_2} \dots q_r^{e_r}.$$

Si les facteurs q_i vérifient

$$q_i \leq B, 1 \leq i \leq r$$

on dit que $p-1$ est B-**lisse**. L'algorithme suivant permet de trouver un facteur p si $p-1$ est B-lisse.

1. On prend $2 \leq a < N$ et on pose $x = a$.
2. Pour $i = 1, 2, \dots s$:
   (a) $x \to x^i \bmod N$ (notons qu'ici on calcule $a^{i!} \bmod N$)

(b) $d := (x-1, N)$

(c) si $1 < d < N$, on a trouvé un facteur d de N

3. retour à la première étape.

Soit $s = max\, e_j q_j$. Alors $q_j^{e_j}$ divise $s!$, i.e. $(p-1)|s!$. On a donc $a^{s!} \equiv 1 \bmod p$. Il est peu probable que $a^{s!} \equiv 1 \bmod N$ et on espère donc trouver un facteur de N.

4.1.2 Algorithme ECM

Courbes elliptiques modulo N

Soit E une courbe elliptique donnée par une équation homogène $Y^2Z = X^3 + aXZ^2 + bZ^3$ où les coefficients $a, b \in \mathbb{Z}/N$ et le derminant $\Delta(E)$ sont inversibles. On définit

$$E(\mathbb{Z}/N) = \{(X:Y:Z), X, Y, Z \in \mathbb{Z}/N, pgcd(N, X, Y, Z) = 1,\ Y^2Z = X^3 + aXZ^2 + bZ^3\}.$$

Si N était premier, on pourrait toujours trouver la somme $P + Q$ pour tous deux points $P, Q \in E(\mathbb{Z}/N)$ par les formules de la loi explicite (Proposition 2.2.5). Dans ces formules on est amenés à inverser $x_P - x_Q$. Si cela n'est pas possible, et si $x_P \neq x_Q$, on a nécessairement que $(x_P - x_Q, N) > 1$ et on trouve donc un facteur de N. On obtient donc l'algorithme suivant. Pour l'efficacité l'on utilise souvent plusieurs courbes à la fois.

L'algorithme

1. On fixe un entier m (souvent $10 < m < 20$) et un entier B (par exemple, d'ordre 10^8).
2. On choisit m courbes elliptiques aléatoires E_i modulo N :

$$E_i : Y^2Z = X^3 + a_iXZ^2 + b_iZ^3$$

et un point $P_i \in E_i$. Pour ce faire, on choisit de façon aléatoire a_i, $P_i = (x_{i,0}, y_{i,0})$ et on pose $b_i = y_{i,0}^2 - x_{i,0}^3 - ax_{i,0}$.

3. Pour tout i on calcule successivement $(B!)P_i$ sur E_i. Si une des opérations d'inversion est impossible, on trouve un facteur de N.
4. Sinon, on change B ou les courbes E_i et on revient à la première étape.

L'opération d'inversion échoue si $B!P_i = O$ dans $E_i(\mathbb{F}_p)$ où p est un facteur de N. C'est le cas si l'ordre $\#E_i(\mathbb{F}_p)$ divise $B!$. Or $\#E_i(\mathbb{F}_p)$ varie dans l'intervalle $]p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}[$, alors que, par exemple, dans la méthode de Pollard, l'ordre $p - 1$ est fixé. On s'attend donc à ce que l'algorithme soit plus efficace.

4.2 L'algorithme de Schoof

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. D'après le théorème de Hasse 3.0.1, le nombre $\#E(\mathbb{F}_q)$ satisfait une inégalité

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

Dans cette section on va décrire un algorithme, du à Schoof, qui permet de calculer $\#E(\mathbb{F}_q)$ en temps $O((log\, q)^c)$, pour c une constante convenable. Soit

$$a_q = q + 1 - \#E(\mathbb{F}_q).$$

Pour determiner a_q on va determiner a_q modulo ℓ pour beaucoup de nombres premiers ℓ.

On prend donc ℓ un premier. Soit $P \in E(\overline{\mathbb{F}}_q)[\ell]$. D'après le théorème 3.3.6, on a

$$a_q\phi_q(P) = \phi_q^2(P) + qP,$$

où ϕ_q es le morphisme de Frobenius. Par ailleurs, comme $\ell P = O_E$, on a

$$[a_q]_\ell\, \phi_q(P) = \phi_q^2(P) + [q]_\ell P, \tag{4.1}$$

où $[a_q]_\ell$ et $[q]_\ell$ sont des restes modulo ℓ. De plus, l'égalité 4.1 détermine $[a_q]_\ell$ de facǫn unique.

D'après la proposition 3.3.7, on a $P \in E(\overline{\mathbb{F}}_q)[\ell] \Leftrightarrow \psi_\ell(P) = O_E$ pour un polynôme ψ_ℓ défini de façon récursive. Ce polynôme est de degré $\frac{\ell^2-1}{2}$. Pour trouver des multiples de P, on peut donc travailler dans l'anneau

$$R_\ell = \mathbb{F}_q[x, y]/(\psi_l(x), y^2 - x^3 - ax - b)$$

de telle sorte qu'on n'a jamais de puissances de y^r pour $r > 1$ et de x^r pour $r > \frac{\ell^2-3}{2}$.

On peut maintenant décrire l'algorithme de Schoof.

L'algorithme

1. Soient $A = 1$, $\ell = 3$.
2. si $A < 4\sqrt{q}$:
   (a) pour $n = 0, \ldots \ell - 1$ on vérifie l'égalité (dans l'anneau R_ℓ) :

   $$(x^{q^2}, y^{q^2}) + [q]_\ell(x, y) = n(x^q, y^q)$$

   Si l'égalité est vérifiée, on sauvegarde $n_\ell = n$ et l'on passe à l'étape suivante.
   (b) On change $A \to \ell A$, et on change ℓ par un nombre premier suivant.
3. On trouve a_q comme unique entier $|a_q| \leq 2q$ tel que $a_q \equiv n_\ell$ pour tout ℓ.

Remarque. À la dernière étape de l'algorithme on utilise le théorème des restes chinois pour trouver a avec les conditions $a_q \equiv n_\ell$. Puisque $A = \prod \ell > 4\sqrt{q}$ et $a_q \in]-2q, +2q[$ par le théorème de Hasse, un tel entier est unique.

4.3 Primalité

Les algorithmes à la base des courbes elliptiques sont utilisés pour tester (et prouver) la primalité de très grands entiers (plus que 20000 chiffres), qui ont déjà passés d'autres tests de primalité. Un des records les plus récents est le nombre

$$(2^{83339}+1)/3$$

qui est donc premier et qui a 25088 chiffres. Cet algorithme marche en temps d'ordre $O((log\, N)^4)$.

On va présenter ici le test de primalité de Goldwasser-Kilian. On y utilise les deux énoncés qui suivent.

Proposition 4.3.1. *Soit N un entier premier à 6 et soit E une courbe à coefficients dans $\mathbb{Z}/N$. Supposons qu'il existe*

(i) un entier m et un premier q, $q|m$ et $q > (\sqrt[4]{N}+1)^2$;

(ii) un point $P \in E(\mathbb{Z}/N)$ tel que $mP = O_E$ et $(m/q)P = (x : y : z)$ avec z inversible dans $\mathbb{Z}/N$.

Alors N est premier.

Démonstration. Supposons que N n'est pas premier : on a donc un facteur premier l de N tel que $l \leq \sqrt{N}$. On note $\bar{E}$ la courbe obtenue en réduisant les coefficients a, b de E modulo l. La réduction modulo l du point P donne un point $\bar{P}$ de $\bar{E}$ d'ordre divisible par q (par la condition (ii)). On a donc $q \leq \#\bar{E}(\mathbb{F}_l) \leq (\sqrt{l}+1)^2$ par le théorème de Hasse. Or $l \leq \sqrt{N}$. On obtient donc une contradiction avec la condition (i). □

Proposition 4.3.2. *Soit N un nombre premier, $(N, 6) = 1$ et soit E une courbe elliptique donnée par une équation homogène $Y^2Z = X^3 + aXZ^2 + bZ^3$ où les coefficients $a, b \in \mathbb{Z}/N$ le derminant $\Delta(E)$ sont inversibles. Soit $m = \#E(\mathbb{Z}/N)$. Supposons qu'il existe un nombre premier q tel que $q|m$ et $q > (\sqrt[4]{N}+1)^2$. Alors il existe un point $P \in E(\mathbb{Z}/N)$ tel que $mP = O_E$ et $(m/q)P = (x : y : z)$ avec z inversible dans $\mathbb{Z}/N$.*

Démonstration. Supposons que pour tout point P de $E(\mathbb{Z}/N)$ on a $(m/q)P = O_E$. Ainsi l'ordre de $E(\mathbb{Z}/N)$ divise m/q. D'après le théorème 3.3.9 on a $E(\mathbb{Z}/N) = \mathbb{Z}/d_1 \oplus \mathbb{Z}/d_2, d_1|d_2$, d'où $d_2|(m/q)$. Comme $m \leq d_2^2$, on obient $m \leq (m/q)^2$. Or $m \leq (\sqrt{N}+1)^2$ par le théorème de Hasse, on obtient une contradiction avec l'hypothèse sur q. □

Comme conséquence des deux propriétés ci-dessus, on obtient donc que si l'on trouve une courbe elliptique E telle que l'ordre m de $E(\mathbb{Z}/N)$ admet un grand facteur premier q (i.e. $q > (\sqrt[4]{N}+1)^2$), alors N est premier si et seulement s'il existe un point $P \in E(\mathbb{Z}/N)$ tel que $mP = O_E$ et $(m/q)P = (x : y : z)$ avec z inversible dans $\mathbb{Z}/N$. Pour une courbe elliptique donnée, on peut utiliser l'algorithme

de Schoof pour determiner son ordre m. Ensuite, pour tester si q est premier, on réitère encore la même procédure. On obtient donc l'algorithme suivant.

L'algorithme

1. On choisit une courbe elliptique E et on calcule $m = \#E(\mathbb{Z}/N)$.
2. On divise m par des petits nombres premiers dont on note m_0 le produit et on cherche $q = m/m_0$ qui vérifie $q > (\sqrt[4]{N} + 1)^2$ et qui passe des tests classiques de primalité. Si cela n'est pas achevé, on revient à la première étape.
3. On choisit $x \in \mathbb{Z}/N$ tel que x^3+ax+b est un carré dans $\mathbb{Z}/N$. On obtient donc un point P de la courbe E. On vérifie si $mP = 0_E$ et $(m/q)P = (x : y : z)$ avec z inversible dans $\mathbb{Z}/N$. Si c'est le cas, on sait que N est premier si q est premier. On revient donc à la première étape avec q à la place de N. Sinon, on change le point P et l'on continue.

4.4 Cryptographie avec les courbes elliptiques

On considère généralement le contexte suivant pour les systèmes cryptographiques à clé publique : deux personnes, Alice et Bob veulent s'échanger des messages de façon sécurisée. Eva veut lire leurs messages, elle a l'accès au canal public de la transmission des messages d'Alice et Bob. Dans ce système, on distingue trois algorithmes de base : l'échange de clés, le chiffrement et la signature numérique. Dans la procédure d'échange de clés, Alice et Bob produisent une clé commune (qui n'est connue que par eux), pour utiliser cette clé dans la suite. La procédure de la signature numérique permet à Bob de s'assurer que le message qu'il reçoit est bien envoyé par Alice. Les schémas que l'on décrit ci-dessous peuvent aussi être utilisés dans n'importe quel groupe. On décrit ensuite des aspects spécifiques aux courbes elliptiques.

4.4.1 L'échange de clés : schéma Diffie-Hellman

1. Données publiques : E une courbe elliptique sur un corps fini $\mathbb{F}_q$ et un point $P \in E(\mathbb{F}_q)$ d'ordre suffisamment grand.
2. Choix secret d'Alice : un entier a.
3. Choix secret de Bob : un entier b.
4. Alice envoie $P_a = aP$ à Bob.
5. Bob calcule $P_b = bP$ et l'envoie à Alice ;
6. Alice calcule $aP_b = abP$ et Bob calcule $bP_a = abP$. La clé commune est une certaine fonction du même point abP.

Définition 4.4.1. On appelle **problème de Diffie-Hellman** le problème suivant :

étant donné P, aP et bP dans $E(\mathbb{F}_q)$, trouver abP.

La difficulté à résoudre ce problème pour une courbe elliptique E garantit la sécurité du schéma Diffie-Hellman.

4.4.2 Cryptosystème ElGamal

Pour recevoir un message d'Alice, Bob choisit une courbe elliptique E sur un corps fini $\mathbb{F}_q$ et point $P \in E$. Il choisit aussi un entier secret s et il calcule $B = sP$. Les données publiques sont les suivantes

$$E, P, B.$$

La clé secrète de Bob est l'entier s.

Pour coder un message, Alice utilise l'algorithme suivant :

1. Elle représente son message comme un point $M \in E(\mathbb{F}_q)$.
2. Elle choisit un entier secret k au hasard et calcule $M_1 = kP$, $M_2 = M + kB$.
3. Alice envoie les points M_1, M_2 à Bob.

Pour retrouver le message d'Alice, Bob calcule

$$M_2 - sM_1 = (M + kB) - s(kP) = M + k(sP) - skP = M.$$

4.4.3 Signature numérique

Le principe de la signature numérique est l'inverse de celui de codage : tout le monde peut vérifier si la signature est correcte, mais seulement Alice peut signer un document. On présente ici l'algorithme que l'on utilise dans le standard ECDSA.

Pour signer son document, Alice choisit une courbe elliptique E sur un corps fini $\mathbb{F}_q$, telle que $\#E(\mathbb{F}_q) = fr$, où r est un grand premier et où f est un entier, généralement $f = 1, 2$ ou 4. Elle choisit un point $P \in E$ d'ordre r. Elle choisit aussi un entier secret s et calcule $Q = sP$. Les informations suivantes

$$E, r, P, Q$$

sont visibles par tous.

Pour signer son message m (qu'on voit comme un entier cette fois-ci), Alice choisit un entier k au hasard et calcule $R = kP = (x, y)$ et $z = k^{-1}(m + sx) \bmod r$. Ensuite Alice signe le document

$$m, R, z.$$

Pour vérifier la signature, Bob utilise la procédure suivante.

1. Il calcule $u_1 = z^{-1}m \bmod r$ et $u_2 = z^{-1}x \bmod r$.
2. Il calcule $V = u_1P + u_2Q$.
3. Il décide que la signature est correcte si $V = R$.

On laisse en exercice la vérification qu'on doit effectivement avoir que $V = R$ si le document est bien signé par Alice.

4.5 Logarithme discret

Définition 4.5.1. Soit G un groupe. Dans le problème du **logarithme discret** dans G on demande de trouver, pour $x, y \in G$ un entier m tel que $x^m = y$ (si un tel entier existe).

La difficulté à resoudre ce problème dans le cas où $G = E(\mathbb{F}_q)$ est la base de la sécurité des algorithmes ci-dessus. En général, pour G un groupe d'odre n, les algorithmes actuels pour résoudre ce problème marchent en temps $O(\sqrt{N})$ (ce qui est beaucoup !). On discute ici briévement deux algorithmes généraux pour le problème du logarithme discret, ainsi qu'un algorithme, dû à Menezes, Okamoto et Vanstone, qui s'applique à certaines courbes elliptiques et utilise l'accouplement de Weil.

4.5.1 Babystep-Giantstep

Soit G un groupe, $x, y \in G$ et soit n l'ordre de x. Soit N un entier $N = \lceil \sqrt{n} \rceil$.

L'algorithme

1. on sauvegarde la liste suivante d'éléments de G : $x, x^2, x^3, \dots x^N$;
2. on pose $z = (x^N)^{-1}$ et on sauvegarde $yz, yz^2, yz^3, \dots yz^N$.
3. on cherche des coïncidences dans ces deux listes : si $x^i = yz^j$, on a trouvé $y = x^{i+jN}$.

Le problème de cet algorithme est qu'on a besoin de suvegarder les deux listes. La méthode de Pollard permet de resoudre ce problème.

4.5.2 ρ-méthode de Pollard

Soient G un groupe, $x, y \in G$ et soit n l'ordre de x. On cherche m tel que $x^m = y$. Pour ce faire, on va trouver des entiers i, j, i_1, j_1 tels que

$$x^i y^j = x^{i_1} y^{j_1}. \tag{4.2}$$

On aura donc $x^{i-i_1} = y^{j_1-j}$, ce qui permet de trouver m si $j - j_1$ est premier à l'ordre de x dans G (ce que l'on peut toujours supposer quitte à se restreindre à x d'ordre premier).

Soit $G = A \cup B \cup C$ l'union disjointe, où A, B, C sont de même cardinal (à quelques éléments près). On pose $f : G \to G$ la fonction

$$f(z) = \begin{cases} xz & z \in A \\ z^2 & z \in B \\ yz & z \in C. \end{cases}$$

Soit $x_0 = x \in G$. Pour tout $i > 1$ on définit $x_i = f(x_{i-1})$. Soit t le plus grand entier tel que x_{t-1} n'apparait qu'une fois dans la suite $(x_i)_{i \geq 0}$ et soit l le plus petit entier tel que $x_{t+l} = x_t$. Alors, on peut montrer que $t + l$ est d'ordre $O(\sqrt{n})$ et qu'il existe $1 \leq i < t + l$ tel que $x_{2i} = x_i$, ce qui permet de trouver la collision 4.2.

4.5.3 L'attaque MOV

Dans l'algorithme de Menezes, Okamoto et Vanstone on réduit le problème de logarithme discret dans $E(\mathbb{F}_q)$ à un problème de logarithme discret dans le groupe $\mathbb{F}_{q^d}$ pour certain d.

Définition 4.5.2. Soit m un entier. Le **degré de plongement** de m dans un corps fini $\mathbb{F}_q$ est le plus petit entier d tel que

$$q^d \equiv 1(\bmod m).$$

Remarque. La condition ci-dessus est équivalente à la condition $\mu_m \subset \mathbb{F}_{q^d}$.

Lemme 4.5.3. *Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$ et soit $m \geq 1$ un entier premier à q et à $q-1$. Soit d le degré de plongement de m dans $\mathbb{F}_q$. Si $E(\mathbb{F}_q)$ contient un point d'ordre exact m, alors $E[m] \subset E(\mathbb{F}_{q^d})$.*

Démonstration. Soit P le point d'ordre exact m et soit $T \in E(\overline{\mathbb{F}}_q)[m]$ tel que $\{P, T\}$ est une base de $E(\overline{\mathbb{F}}_q)[m] = \mathbb{Z}/m \oplus \mathbb{Z}/m$. Soit ϕ_q l'endomorphisme de Frobenius. On a

$$\phi_q(P) = P, \phi_q(T) = uP + vT, u, v \in \mathbb{Z}/m.$$

D'après les propriétés de l'accouplement de Weil

$$e_m(P,T)^q = e_m(\phi_q(P), \phi_q(T)) = e_m(P,P)^u e_m(P,T)^v = e_m(P,T)^v.$$

Puisque $e_m(P,T)$ est une racine ℓ-ième primitive de l'unité (proposition 3.3.11), on en déduit que $v \equiv q \,(\bmod m)$, i.e.

$$\phi_q(T) = uP + qT.$$

On en déduit

$$\phi_{q^d}(T) = u(1 + q + q^2 + \ldots + q^{d-1})P + q^d T.$$

Par définition de d, on a $q^d \equiv 1 \,(\bmod m)$, d'où $q^d T = T$ et $(1+q+q^2+\ldots+q^{d-1})P = O_E$. On a donc $\phi_{q^d}(T) = T$, d'où $T \in E(\mathbb{F}_{q^d})$.

□

L'algorithme

Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$ et soit m un entier, $(m, q) = 1$. Soient P, Q deux points d'ordre m et soit d le degré de plongement de m dans $\mathbb{F}_q$.

1. On prend $T \in E(\overline{\mathbb{F}}_q)[m]$ tel que P, T engendrent $E[m]$ (voir 3.3.8). D'après le lemme ci-dessus, $T \in E(\mathbb{F}_{q^d})$.
2. D'après la proposition 3.3.11, $e_m(P,T)$ est une racine m-ième primitive de l'unité. D'après la définition de d, on a $e_m(P,T) \in \mathbb{F}_{q^d}$. On dispose des algorithmes pour calculer l'accouplement de Weil (dans $E(\mathbb{F}_{q^d})$) : on trouve

alors $e_m(Q,T)$. Puisque $e_m(P,T)$ est une racine n-ième primitive de l'unité, on a que

$$Q = rP \Leftrightarrow e_m(Q,T) = e_m(P,T)^r.$$

On trouve donc le problème de logarithme discret dans $\mathbb{F}_{q^d}$.

4.5.4 Courbes supersingulières

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de caractéristique $p \geq 5$. Rappelons (cf. théorème 3.3.8) que le groupe $E(\bar{\mathbb{F}}_p)[p]$ est soit réduit à un point O_E, soit $E(\bar{\mathbb{F}}_p)[p] \simeq \mathbb{Z}/p$.

Définition 4.5.4. On dit que E est **supersingulière** si $E(\bar{\mathbb{F}}_p)[p] = \{O_E\}$.

Proposition 4.5.5. *Soit $a = q + 1 - \#E(\mathbb{F}_q)$. Les assertions suivantes sont équivalentes :*
(i) E est supersingulière ;
(ii) $a \equiv 0 \ (mod\ p)$;
(iii) $\#E(\mathbb{F}_q) \equiv 1 \ (mod\ p)$.

Démonstration. Soient α, β les racines du polynôme $x^2 - ax + q = 0$. Soit $s_n = \alpha^n + \beta^n$. On a $s_0 = 2, s_1 = a$ et on vérifie par récurrence :

$$s_{n+1} = as_n - qs_{n-1}.$$

D'après la définition de a, on a $(ii) \Leftrightarrow (iii)$.

Supposons (ii). On a alors $s_n \equiv 0 \pmod p$, d'où $\#E(\mathbb{F}_{q^n}) \equiv 1 \pmod p$ pour tout n (cf. théorème 3.3.6). On n'a donc pas de point d'ordre p dans le groupe $E(\mathbb{F}_{q^n})$, d'où (i).

Supposons que E est supersingulière. Supposons que $a \neq 0 \pmod p$. On a donc $s_{n+1} \equiv as_n \pmod p$ et

$$\#E(\mathbb{F}_q) = q^n + 1 - s_n \equiv 1 - a^n \pmod p.$$

Ainsi, pour $n = p-1$ on obtient que $p | \#E(\mathbb{F}_q)$ et donc E n'est pas supersingulière. Contradiction. □

Corollaire 4.5.6. *Une courbe elliptique E sur $\mathbb{F}_p$ est supersingulière si et seulement si $\#E(\mathbb{F}_p) = p + 1$.*

Démonstration. D'après le théorème de Hasse, $|a| \leq 2\sqrt{p}$. Dans la proposition précédente on a donc $a = 0 \Leftrightarrow a \equiv 0 \pmod p \Leftrightarrow \#E(\mathbb{F}_p) = p + 1$. □

Corollaire 4.5.7. *Supposons que $p \equiv 2 \ (mod\ 3)$. Soit $b \in \mathbb{F}_p$ non nul. La courbe elliptique $y^2 = x^3 + b$ sur $\mathbb{F}_p$ est supersingulière.*

Démonstration. D'après la section 3.2.1, la condition (iii) de la proposition ci-dessus est satisfaite. □

De point de vue algorithmique, les opérations artihmétiques sur les courbes supersingulières se calculent très facilement. Supposons $a = 0$. On a alors pour tout $P = (x, y) \in E(\bar{\mathbb{F}}_p)$:

$$q(x, y) = -\phi_q(x, y) = (x^{q^2}, -y^{q^2}).$$

Soit m un entier. Pour calculer mP, on procède comme suit :

1. on décompose $m = m_0 + m_1 q + m_2 q^2 + \ldots + m_r q^r$ avec $0 \leq m_i < q$;
2. on calcule $m_i P = (x_i, y_i)$, puis $q^i m_i P = (x_i^{q^{2i}}, (-1)^i y_i^{q^{2i}})$, en enfin on calcule la somme de tous ces points.

Par ailleurs, comme le montre la proposition ci-dessous, l'attaque MOV s'applique à E et le problème de logarithme discret sur E peut être réduit au logartihme discret dans $\mathbb{F}_{q^2}$, ce qui est beaucoup plus simple.

Proposition 4.5.8. *Soit E une courbe elliptique supersingulière sur $\mathbb{F}_q$ et soit $N > 0$ un entier. Supposons $a = q + 1 - \#E(\mathbb{F}_q) = 0$. S'il existe un point $P \in E(\mathbb{F}_q)$ d'ordre N, alors $E(\bar{\mathbb{F}}_q)[N] \subset E(\mathbb{F}_{q^2})$.*

Démonstration. Soit $Q \in E(\bar{\mathbb{F}}_q)[N]$. Puisque $\#E(\mathbb{F}_q) = q+1$, on a $N|q+1$. Puisque E est supersingulière et $a = 0$, on a $\phi_q^2(S) = -qS = S$. Ainsi Q est fixé par ϕ_{q^2}, d'où $Q \in E(\mathbb{F}_{q^2})$. □

4.6 Exercices

1. (a) Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$ et soient $P, Q \in E(\mathbb{F}_q)$. Supposons que le point P est d'ordre n. Montrer que Q est un multiple de P si et seulement si $nQ = O_E$ et $e_n(P, Q) = 1$.

   (b) Soit E une courbe elliptique $y^2 = x^3 + 1$ sur un corps fini $\mathbb{F}_q$, $q \equiv 2 \pmod 3$ et soient $P, Q \in E(\mathbb{F}_q)$. Supposons que le point P est d'ordre n, $(n, 3) = 1$. Soit ζ une racine cubique primitive de l'unité.

      i. Montrer que $\beta : E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})$, $(x, y) \mapsto (\zeta x, y)$ est un automorphisme de E et que $\beta(P)$ est d'ordre n.

      ii. On définit un accouplement de Weil modifié par

      $$\tilde{e}_n(P_1, P_2) = e_n(P_1, \beta(P_2)).$$

      Montrer que $\tilde{e}_n(P, P)$ est une racine n-ième primitive de l'unité.

      iii. En déduire le critère suivant pour résoudre le problème de décision de Diffie-Hellman pour la courbe E :

étant donné P, aP, bP, Q on a $Q = abP \Leftrightarrow nQ = O_E, e_n(P,Q) = 1$ et $\tilde{e}_n(aP, bP) = \tilde{e}_n(Q, P)$.

(c) En utilisant l'accouplement modifié $\tilde{e}_n$, construire un algorithme d'échange de clés pour trois personnes : Alice, Bob et Carl choisissent des entiers secrets a, b, c et calculent $A = aP$, $B = bP$ et $C = cP$. Les données publiques sont les points P, A, B, C. Quelle valeur commune peuvent-ils calculer en utilisant leurs clés ?

(d) Construire un algorithme de la signature numérique : Alice choisit un entier secret a et calcule $A = aP$. Le point A est la donnée publique. Pour signer un document représenté par un point D, Alice calcule $S = aD$. Comment Bob peut vérifier sa signature ?

2. Soit E la courbe elliptique $y^2 = x^3 + b$ définie sur un corps fini $\mathbb{F}_p$, $p \equiv 2 \pmod 3$.

(a) Soit n un entier (n,p)=1. Supposons $E[n](\overline{\mathbb{F}_p}) \subset E(\mathbb{F}_p)$. Montrer que $n|p-1$ et $n^2|p+1$. En déduire $n \leq 2$.

(b) Montrer que $E[2] \nsubseteq E(\mathbb{F}_p)$.

(c) Montrer que le groupe $E(\mathbb{F}_p)$ est cyclique. Quel est l'ordre de ce groupe ?

3. Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$.

(a) Montrer qu'une application α de $E(\mathbb{F}_p)$ dans lui-même est injective si et seulement si elle est surjective (α n'est pas nécessairement un endomorphisme).

(b) Montrer que si $E(\mathbb{F}_q)$ n'a pas de point d'ordre n, alors $E(\mathbb{F}_q)/nE(\mathbb{F}_q) = 0$.

4. Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. Supposons $E(\mathbb{F}_q) = \mathbb{Z}/n \oplus \mathbb{Z}/mn$.

(a) Montrer que $n|q-1$. En déduire que l'on peut écrire

$$q = mn^2 + kn + 1 \tag{4.3}$$

pour certain entier k.

(b) Montrer que $mn \geq \sqrt{m}(\sqrt{q} - 1)$ et que $|k| \leq 2\sqrt{m}$.

(c) Montrer que si $m \geq 17$ et q est suffisamment grand, alors $E(\mathbb{F}_q)$ admet un point d'ordre $N > 4\sqrt{q}$.

(d) Soit $m \geq 1$ fixé. Montrer que, presque tout entier q, qui est une puissance d'un nombre premier, n'est pas de la forme (4.3). (on pourrait utiliser que d'après le théorème des nombres premiers, le nombre des $q = p^r$ avec p premier, $r > 0$ (non fixés) tels que $q \leq x$ est environ $x/log\, x$.)

(e) Montrer que pour presque tout q, une courbe elliptique sur $\mathbb{F}_q$ admet un point d'ordre $N > 4\sqrt{q}$.

5. Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique définie sur un corps fini $\mathbb{F}_p$, $E(\mathbb{F}_p) = \mathbb{Z}/m \oplus \mathbb{Z}/M$, $m|M$. Pour $d \in \mathbb{F}_p$ non carré on définit un *twist* de E est une courbe elliptique E' donnée par une équation $y^2 = x^3 + ad^2x + bd^3$. Soient $a = p + 1 - \#E(\mathbb{F}_p)$ et $a' = p + 1 - \#E'(\mathbb{F}_p)$. On écrit aussi $E'(\mathbb{F}_p) = \mathbb{Z}/n \oplus \mathbb{Z}/N$, où $n|N$.

(a) Montrer qu'après un changement linéaire en coordonnées on peut écrire E' sous la forme $dy^2 = x^3 + ax + b$. En déduire que $a = -a'$.

(b) Montrer que $(m^2, n^2)|2a$.

(c) Montrer que $a \equiv 2 (\text{mod } m)$ et que $a \equiv -2 (\text{mod } n)$ (on pourra utiliser que $E(\overline{\mathbb{F}}_p)[m] \subset E(\mathbb{F}_p)$).

(d) En déduire que $(m^2, n^2)|4$.

(e) Montrer que la restriction du Frobenius ϕ_p sur $E'(\overline{\mathbb{F}}_p)[n^2]$ est donnée par une matrice $\left(\begin{smallmatrix} 1+sn & tn \\ un & 1+vn \end{smallmatrix}\right)$ avec $a \equiv 2 + (s+v)n \ (\text{mod } n^2)$ et $p \equiv 1 + (s+v)n \ (\text{mod } n^2)$. En déduire que $4p \equiv a^2 (\text{mod } n^2)$.

(f) Montrer que $\frac{m^2 n^2}{4} \leq 4p - a^2$.

(g) En déduire que pour p suffisamment grand, soit la courbe E, soit la courbe E' admet un point d'ordre plus grand que $4\sqrt{p}$.

6. Soit $E : y^2 = x^3 - x + 19$ une courbe elliptique sur $\mathbb{F}_{23}$.

(a) Montrer que $P = (2, 5)$ est bien un point de E. En admettant que $4P = (-2, 6)$, calculer $8P$, puis $9P$. En déduire que $17P = O_E$.

(b) Montrer que $\#E(\mathbb{F}_{23}) < 34$. En déduire le cardinal de $E(\mathbb{F}_{23})$ et donner les générateurs de ce groupe.

(c) Que vaut $\#E(\mathbb{F}_{23^2})$?

Chapitre 5

Courbes elliptiques sur les corps de nombres

5.1 Généralités sur les corps de nombres

5.1.1 Rappels sur les corps de nombres et l'anneau des entiers

On commence par rappeler quelques notions et résultats fondamentaux sur les corps de nombres (voir le cours MAT552).

Définition 5.1.1. Un **corps de nombres** est une extension algébrique finie du corps des nombres rationnels $\mathbb{Q}$.

Pour la suite de ce paragraphe on fixe un corps de nombres K.

Par le théorème de l'élément primitif, on peut écrire $K = \mathbb{Q}(\alpha)$ avec $[K : \mathbb{Q}] = n = \deg P$, où P est le polynôme minimal de α. Supposons que P possède r_1 racines réelles $\alpha_1, \dots \alpha_{r_1}$ et r_2 paires de racines complexes $\alpha_{r_1+1}, \bar{\alpha}_{r_1+1}, \dots, \alpha_{r_1+r_2}, \bar{\alpha}_{r_1+r_2}$. On a donc r_1 plongements de K dans $\mathbb{R}$ définis par $\sigma_i(\alpha) = \alpha_i$ et r_2 paires de plongements de K dans $\mathbb{C}$: $\sigma_j(\alpha) = \alpha_{r_1+j}$ et $\bar{\sigma}_j(\alpha) = \bar{\alpha}_{r_1+j}$. On dit que K a r_1 **plongements réels et** r_2 **paires de plongements complexes.** On définit le plongement canonique

$$\tau_K : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$
$$\tau_K(x) = (\sigma_i(x))_{i=1,\dots,r_1+r_2}.$$

Définition 5.1.2. L'anneau des **entiers** de K est l'anneau

$\mathcal{O}_K = \{x \in K$ est une racine d'un polynôme unitaire à coefficients entiers$\}$.

Exemples.

1. Si $K = \mathbb{Q}(\sqrt{d})$, où d n'a pas de facteurs carrés, alors $\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{si } d \equiv 2,3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{si } d \equiv 1 \bmod 4. \end{cases}$
2. Plus généralement, si $[K : \mathbb{Q}] = n$, alors on peut trouver $e_1, \dots e_n \in \mathcal{O}_K$ tels que
$$\mathcal{O}_K = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_n.$$
3. Supposons que K a r_1 plongements réels et r_2 paires de plongements complexes. Si $\alpha \in \mathcal{O}_K$, alors le polynôme $\chi_{\alpha,K} = \prod_{i=1}^{r_1}(x - \sigma_i(\alpha)) \prod_{j=1}^{r_2}(x - \sigma_{r_1+j}(\alpha))(x - \bar{\sigma}_{r_1+j}(\alpha))$ est à coefficients entiers : $\chi_{\alpha,K} \in \mathbb{Z}[x]$.

On a le théorème fondamental suivant, qui est aussi utilisé pour démontrer la finitude du groupe des classes d'idéaux, comme rappelé ci-dessous.

Théorème 5.1.3. *L'image $\tau_K(\mathcal{O}_K)$ est un réseau de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.*
Autement dit, $D := \tau_K(\mathcal{O}_K)$ est un sous-groupe discret de $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ (i.e. pour tout réel $r > 0$ l'ensemble $\{v \in D, |v| \leq r\}$ est fini) et engendre V comme $\mathbb{R}$-espace vectoriel.

Définition 5.1.4. Soient I, J deux idéaux dans $\mathcal{O}_K$. On dit que I et J sont **équivalents** s'il existe $\alpha, \beta \in \mathcal{O}_K$ non nuls, tels que
$$\alpha I = \beta J.$$

Théorème 5.1.5. *Tout idéal I de $\mathcal{O}_K$ est inversible : il existe $\alpha \in \mathcal{O}_K$ non nul et un idéal $J \subset \mathcal{O}_K$ tels que $IJ = \alpha\mathcal{O}_K$. L'ensemble des classes d'ideaux forme un groupe Cl_K. Ce groupe est fini.*

Théorème 5.1.6. *(i) Tout idéal premier non nul de $\mathcal{O}_K$ est maximal.*
(ii) Tout idéal I de $\mathcal{O}_K$ se décompose de manière unique (à une permutation près) en produit des idéaux premiers.

Remarque.
1. On montre que l'anneau $\mathcal{O}_K$ est un anneau de Dedekind : c'est un anneau noethérien, intégralement clos et tel que tout idéal premier non nul est maximal.
2. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. L'unicité de la décomposition dans (ii) implique en particulier que les inclusions $\mathfrak{p}^{m+1} \subset \mathfrak{p}^m$ sont strictes.

En particulier, si p est un premier, on peut écrire
$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}$$

avec $\mathfrak{p}_i$, $i = 1, \ldots, m$ des idéaux premiers distincts et $e_i \geq 1$. Le corps $\mathcal{O}_K/\mathfrak{p}_i$ est une extension finie du corps $\mathbb{F}_p$, on pose $f_{\mathfrak{p}_i} = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$. En particulier,

$$N\mathfrak{p}_i := card(\mathcal{O}_K/\mathfrak{p}_i) = p^{f_{\mathfrak{p}_i}}.$$

Rappelons que si $n = [K : \mathbb{Q}]$, on a

$$n = \sum_{i=1}^{m} e_i f_{\mathfrak{p}_i}.$$

En effet, cela découle de l'égalité

$$p^n = N(p\mathcal{O}_K) = N\mathfrak{p}_1^{e_1} \cdot \ldots \cdot N\mathfrak{p}_m^{e_m} = p^{\sum e_i f_{\mathfrak{p}_i}}.$$

Soit I un idéal de $\mathcal{O}_K$ et soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Le théorème 5.1.6 permet de définir

$$\mathrm{ord}_{\mathfrak{p}}(I) = max\{n \geq 0 \,|\, I \subset \mathfrak{p}^n.\}$$

Si $x \in \mathcal{O}_K$, on définit $\mathrm{ord}_{\mathfrak{p}}(x)$ comme l'odre en $\mathfrak{p}$ de l'idéal (x) et on prolonge cette notion pour tout $x \in K$.

5.1.2 Valeurs absolues

Définition 5.1.7. Soit K un corps. Une **valeur absolue** v sur K est une application

$$|\cdot|_v : K \to \mathbb{R}_+$$

telle que

(i) $|x|_v = 0$ si et seulement si $x = 0$;

(ii) $|xy|_v = |x|_v|y|_v$ pour tous $x, y \in K$;

(iii) il existe une constante $C > 0$ telle que $|x+y|_v \leq C \max\{|x|_v, |y|_v\}$ pour tous $x, y \in K$. Si $C = 1$, on dit que la valeur absolue est **ultramétrique**.

Remarque. On vérifie facilement que si $|\cdot|_v$ est une valeur absolue sur un corps F, alors $|\cdot|_v^\alpha$ est aussi une valeur absolue sur F pour tout $\alpha > 0$.

Places finies. Pour tout idéal premier $\mathfrak{p}$ d'un corps de nombres K on définit une valeur absolue sur K par

$$|x|_{\mathfrak{p}} = N\mathfrak{p}^{-ord_{\mathfrak{p}}(x)}$$

On note $\Sigma_{fini}(K)$ l'ensemble de ces valeurs absolues. On vérifie que ces valeurs absolues sont ultramétriques.

Places de K. Supposons que K a r_1 plongements réels et r_2 paires de plongements complexes. Pour $\sigma_i : K \hookrightarrow \mathbb{R}$, $i = 1, \dots r_1$, on définit une valeur absolue par

$$|x|_{\sigma_i} = |\sigma_i(x)|$$

et pour $\sigma_j : K \hookrightarrow \mathbb{C}, j = 1, \dots r_2$ on définit une valeur absolue

$$|x|_{\sigma_j} = |\sigma_j(x)|^2.$$

On note $\Sigma_\infty(K)$ l'ensemble de ces $r_1 + r_2$ valeurs absolues.

On pose $\Sigma(K) = \Sigma_{fini}(K) \cup \Sigma_\infty(K)$ l'ensemble des **places** de K.

Théorème 5.1.8. [Formule du produit] *Soit $x \in K^*$. Alors on a*

$$\prod_{v \in \Sigma(K)} |x|_v = 1.$$

Démonstration. Supposons d'abord que $K = \mathbb{Q}$. On peut alors écrire $x = \pm p_1^{e_1} \dots p_r^{e_r}$ avec p_i premiers et $e_i \in \mathbb{Z} \setminus \{0\}, i = 1, \dots m$. On a donc $|x|_{p_i} = p_i^{-e_i}$ pour des places finies et pour la place ∞ correspondante au plongement $\mathbb{Q} \subset \mathbb{R}$, on a $|x|_\infty = |x| = p_1^{e_1} \dots p_r^{e_r}$. On a donc

$$\prod_{v \in \Sigma(\mathbb{Q})} |x|_v = p_1^{-e_1} \cdot \dots \cdot p_r^{-e_r} p_1^{e_1} \dots p_r^{e_r} = 1.$$

Dans le cas général, soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Écrivons

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}.$$

Soit $x \in K^*$ et soit $N_{K/\mathbb{Q}}(x) \in \mathbb{Q}$ la norme de x. On a alors

$$\prod_{\mathfrak{p}|p} |x|_\mathfrak{p} = |N_{K/\mathbb{Q}}(x)|_p. \tag{5.1}$$

En effet, on vérifie que $N_{K/\mathbb{Q}}(x) = \pm N(x\mathcal{O}_K)$, d'où

$$N_{K/\mathbb{Q}}(x) = \pm \prod_\mathfrak{p} N\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)} = \pm \prod p^{\sum_{\mathfrak{p}|p} f_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(x)}.$$

On en déduit

$$|N_{K/\mathbb{Q}}(x)|_p = p^{-\sum_{\mathfrak{p}|p} f_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(x)} = \prod_{\mathfrak{p}|p} N\mathfrak{p}^{-\mathrm{ord}_\mathfrak{p}(x)} = \prod_{\mathfrak{p}|p} |x|_\mathfrak{p},$$

d'où on obtient (5.1).

Pour les places à l'infini on a également

$$\prod_{v\in\Sigma_\infty(K)} |x|_v = |N_{K/\mathbb{Q}}(x)|_\infty.$$

En effet, par la définition de la norme $N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=1}^{r_2} \sigma_{i+j}(x)\bar{\sigma}_{i+j}(x)$, d'où

$$|N_{K/\mathbb{Q}}(x)|_\infty = \prod_{v\in\Sigma_\infty(K)} |x|_v.$$

On a donc, en regroupant des places de K au-dessus des places de $\mathbb{Q}$:

$$\prod_{v\in\Sigma(K)} |x|_v = \prod_{w\in\Sigma(\mathbb{Q})} \prod_{v|w} |x|_v = \prod_{w\in\Sigma(\mathbb{Q})} N_{K/\mathbb{Q}}(x)_w = 1$$

d'après le premier cas où $K = \mathbb{Q}$.

□

5.2 Hauteurs

5.2.1 Hauteurs de Weil sur $\mathbb{P}^n(\overline{\mathbb{Q}})$

La notion de hauteur a pour but de donner une mesure pour la taille d'un point d'un espace projectif ou d'une variété algébrique projective définie sur un corps de nombres K.

Définition 5.2.1. Soit K un corps de nombres et soit $P = (x_0 : \ldots : x_n)$ un point de $\mathbb{P}^n_K$. On définit la hauteur de P relative au corps K par la formule

$$H_K(P) = \prod_{v\in\Sigma(K)} \max(|x_0|_v, \ldots |x_n|_v).$$

Remarque.

1. D'après la formule de produit 5.1.8, cette définition ne dépend pas du choix des coordonnées homogènes du point P.
2. Si $K = \mathbb{Q}$, on peut trouver des coordonnées $P = (x_0 : \ldots : x_n)$ avec x_i entiers premiers entre eux. On a alors $H_\mathbb{Q}(P) = \max(|x_0|, \ldots, |x_n|)$.

Lemme 5.2.2. *Soit L/K une extension finie des corps de nombres de degré d. Si $P \in \mathbb{P}^n(K)$, alors*

$$H_L(P) = H_K(P)^d.$$

Démonstration. Soit $P = (x_0 : \ldots : x_n)$. On a alors

$$H_L(P) = \prod_{w \in \Sigma(L)} \max_{\mathrm{i}} |x_i|_w = \prod_{v \in \Sigma(K)} \prod_{w|v} \max_{\mathrm{i}} |x_i|_w =$$
$$= \prod_{v \in \Sigma(K)} \max_{\mathrm{i}} |x_i|_v^{\sum_{w|v} e_w f_w} = \prod_{v \in \Sigma(K)} \max_{\mathrm{i}} |x_i|_v^d = H_K(P)^d.$$

□

Le lemme précédent permet de définir la hauteur de Weil sur $\mathbb{P}^n(\overline{\mathbb{Q}})$.

Définition 5.2.3. La **hauteur de Weil** sur $\mathbb{P}^n(\overline{\mathbb{Q}})$ est l'application

$$H : \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{R}$$
$$P \in \mathbb{P}^n(K) \mapsto H_K(P)^{1/[K:\mathbb{Q}]}.$$

On pose $h_K = logH_K$ et $h = logH$.

Définition 5.2.4. Si K est un corps de nombres et $x \in K$, on définit

$$H(x) = H(1 : x).$$

L'énoncé suivant affirme la finitude du nombre de points de hauteur bornée.

Théorème 5.2.5. [Northcott, Kronecker] *Soient $d \geq 1$, $C > 0$.*

(i) L'ensemble

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}), [\mathbb{Q}(P) : \mathbb{Q}] \leq d, H(P) \leq C\}$$

est fini.

(ii) On a $H(P) > 1$, sauf si $P = (x_0 : \ldots : x_n)$ est tel que pour tout i soit x_i est une racine de l'unité, soit $x_i = 0$.

Démonstration. (i) Soit $P = (x_0 : \ldots : x_n)$. Quitte à permuter, on peut supposer $x_0 \neq 0$ et écrire $P = (1 : \alpha_1 \ldots : \alpha_n)$ avec $\alpha_i \in \overline{\mathbb{Q}}$. D'après la définition

$$H(\alpha_i) \leq H(P) \text{ et } [\mathbb{Q}(\alpha_i) : \mathbb{Q}] \leq [\mathbb{Q}(P) : \mathbb{Q}].$$

Il suffit donc de montrer que l'ensemble

$$S = \{\alpha \in \overline{\mathbb{Q}}, [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d, H(\alpha) \leq C\}$$

est fini. D'après la partie (ii) du lemme ci-dessous, les coefficients du polynôme minimal sont bornés pour tout $\alpha \in S$, ce qui montre bien que l'ensemble S est fini.

(ii) On écrit $P = (1 : \alpha_1 \ldots : \alpha_n)$ comme ci-dessus. Si $H(P) \leq 1$, alors $|\alpha_i|_v \leq 1$ pour tout i et tout v. Cette dernière condition est aussi vérifiée pour α_i^m pour tout entier $m > 0$. D'après (i) l'ensemble $\{(1 : \alpha_1^m \ldots : \alpha_n^m)\}$ est fini, et donc α_i sont des racines de l'unité.

□

Lemme 5.2.6. *(i) [Lemme de Gauss] Soit K un corps de nombres et soient $P, Q \in K[x]$. Soit v une valeur absolue correspondant à un idéal premier $\mathfrak{p}$ de K et soit $||P||_v$ est la norme sup des coefficients de P. Alors $||PQ||_v = ||P||_v||Q||_v$.*

(ii) Soit $\alpha \in \overline{\mathbb{Q}}$ et soit $K = \mathbb{Q}(\alpha)$. Soit $P \in \mathbb{Z}[x]$, $P(x) = a_0(x - \alpha_1)\ldots(x - \alpha_d)$ le polynôme minimal de α. Alors

$$H_K(\alpha) = |a_0| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

Démonstration. (i) Soit $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ (cf. la remarque après le théorème 5.1.6 pour voir que cet ensemble est non vide). On a en particulier $\mathrm{ord}_{\mathfrak{p}}(\pi) = 1$. Quitte à multiplier les coefficients de P et Q par une puissance convenable de π, on peut donc supposer que $||P||_v = ||Q||_v = 1$. En particulier, les images $\bar{P}$ et $\bar{Q}$ de P et Q dans l'anneau $\mathcal{O}/\mathfrak{p}[x]$ ne sont pas nulles. Puisque $\mathcal{O}/\mathfrak{p}[x]$ est un anneau intègre, on en déduit que $\bar{P}\bar{Q} = \overline{PQ}$ est non nul, ce qui signifie que $||PQ||_v = 1$.

(ii) Soit $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$. On a par définition de la hauteur :

$$H_K(\alpha)^{[L:K]} = H_L(\alpha) = \prod_{w \in \Sigma_{fini}(L)} \max(1, |\alpha|_w) \prod_{w \in \Sigma_\infty(L)} \max(1, |\alpha|_w). \quad (5.2)$$

Pour les places à l'infini on a :

$$\prod_{w \in \Sigma_\infty(L)} \max(1, |\alpha|_w) = \prod_{v \in \Sigma_\infty(K)} \max(1, |\alpha|_v)^{[L:K]} = (\prod_{i=1}^{d} \max(1, |\alpha_i|))^{[L:K]}. \quad (5.3)$$

Soit $w \in \Sigma_{fini}(L)$. D'après le lemme de Gauss (i) appliqué à P on a

$$1 = ||P||_w = |a_0|_w \prod_{i=1}^{d} \max(1, |\alpha_i|_w).$$

De plus, d'après la formule de produit,

$$\prod_{w \in \Sigma_{fini}(L)} |a_0|_w = |a_0|^{-[L:\mathbb{Q}]}.$$

Pour les places finies on a a donc :

$$1 = \prod_{w \in \Sigma_{fini}(L)} |a_0|_w \prod_{i=1}^{d} \prod_{w \in \Sigma_{fini}(L)} \max(1, |\alpha_i|_w) = |a_0|^{-[L:\mathbb{Q}]} (\prod_{w \in \Sigma_{fini}(L)} \max(1, |\alpha|_w))^d. \quad (5.4)$$

On déduit alors le résultat de (5.3), (5.4) et (5.2) :

$$H_K(\alpha)^{[L:K]} = |a_0|^{[L:\mathbb{Q}]/d}(\prod_{i=1}^{d} \max(1, |\alpha_i|))^{[L:K]}.$$

□

Théorème 5.2.7. *Soit $(P_0, \dots P_m), P_i \in \bar{\mathbb{Q}}[x_0, \dots x_n], i = 0, \dots m$ une famille de polynômes homogènes de degré d. Soit $Z = V_p(P_0, \dots P_m) \subset \mathbb{P}^n_{\overline{\mathbb{Q}}}$ et soit $U = \mathbb{P}^n_{\overline{\mathbb{Q}}} \setminus Z$. Soit $V \subset \mathbb{P}^n_{\overline{\mathbb{Q}}}$ une variété projective telle que $V \cap Z = \emptyset$. On définit*

$$\Phi : U(\overline{\mathbb{Q}}) \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$$
$$x \mapsto (P_0(x) : \dots P_m(x)).$$

Alors il existe des constantes c_1, c_2, c_3 qui ne dépendent que de Φ, telles que
(i) pour tout $x \in U(\overline{\mathbb{Q}})$ on a $H(\Phi(x)) \leq c_1 H(x)^d$;
(ii) pour tout $x \in V(\overline{\mathbb{Q}})$ on a $c_2 H(x)^d \leq H(\Phi(x)) \leq c_3 H(x)^d$;

Démonstration. (i) Soit $x \in U(\overline{\mathbb{Q}})$. Il existe K un corps de nombres tel que $x \in U(K)$. On écrit $P_i(x) = \sum_{j=1}^{N} a_{ij} x^j$ où N est le nombre de monômes $x^j = x_0^{i_0} \dots x_n^{i_n}$ de degré d. Soit $v \in \Sigma(K)$. D'après l'inégalité triangulaire pour v, il existe une constante N_v telle que

$$|y_1 + \dots + y_N|_v \leq N_v \max(|y_1|_v, \dots, |y_N|_v). \tag{5.5}$$

Notons que l'on peut prendre $N_v = 1$ pour toute place finie v. On a donc

$$|P_i(x)|_v \leq N_v \max_j |a_{ij}|_v \max_i |x_i|_v^d. \tag{5.6}$$

Soit $A_v = \max_{i,j} |a_{ij}|$. Notons que $A_v = 1$ sauf pour un nombre fini de places v. On obtient

$$H_K(\Phi(x)) = \prod_v \max_i |P_i(x)|_v \leq \prod_v N_v A_v \max_i |x_i|_v^d = (\prod_v N_v A_v) H_K(x)^d$$

et donc $c_1 = (\prod_v N_v A_v)^{1/[K:\mathbb{Q}]}$ convient.

(ii) Soit $V = V(Q_1, \dots, Q_r)$. Puisque $V \cap Z = \emptyset$, d'après le Nullstellensatz projectif, il existe $M > 0$ et des polynomes A_{ij} et B_{ij} tels que

$$x_j^M = \sum A_{ij} P_i + \sum B_{ij} Q_i.$$

Notons que l'on peut supposer que les polynômes A_{ij} sont homogènes de degré $M - d$. Quitte à remplacer K par une extension finie, on peut aussi supposer que tous les polynômes dans les égalités ci-dessus sont à coefficients dans K. On a donc, pour tout $x = (x_0, \dots x_n) \in V$:

$$|x_j|_v^M = |\sum A_{ij} P_i|_v \leq (m+1)_v \max_i |A_{ij}(x)|_v \max_i |P_i(x)|_v,$$

où $(m+1)_v$ sont des constantes définies commes dans (5.5). En appliquant les inégalités 5.6 à des polynômes A_{ij} qui sont homogènes de degré $M-d$ on peut donc écrire

$$|x_j|_v^M \leq A'_v \max_i |x|_v^{M-d} \max_i |P_i(x)|_v$$

avec des constantes A'_v convenables et telles que $A'_v = 1$ sauf pour un nombre fini de places. On en déduit

$$\max_j |x_j|_v^d \leq A'_v \max_i |P_i(x)|_v,$$

d'où l'inégalité de l'énoncé, en prenant le produit sur v.

□

Remarque. Dans les conditions du théorème précédent on peut écrire $h(\Phi(x)) = dh(x) + \mathcal{O}(1)$.

5.2.2 Hauteur de Weil sur une courbe elliptique

Soit $E \subset \mathbb{P}^2_{\overline{\mathbb{Q}}}$ une courbe elliptique définie par une équation

$$Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{5.7}$$

Pour $P \in E(\overline{\mathbb{Q}})$ on définit

$$h(P) = \begin{cases} h(x_P), & P \neq 0_E \\ 0, & P = 0_E. \end{cases}$$

Théorème 5.2.8. *Il existe une constante c_1 telle que pour tout $P \in E(\overline{\mathbb{Q}})$ on a*

$$-c_1 \leq h(2P) - 4h(P) \leq c_1.$$

Démonstration. L'énoncé est immédiat si $P = 0$ ou un point de 2-torsion. Supposons $x_{2P} \neq 0$. D'après le lemme 5.2.10 ci-dessous, les polynômes $P_0(T,X) = 4T(X^3 + aXT^2 + bT^3)$ et $P_1(T,X) = X^4 - 2aX^2T^2 - 8bXT^3 + a^2T^4$ n'ont pas de zéro commun dans $\mathbb{P}^1$. On applique le théorème 5.2.7(i) à $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$, $\Phi = (P_0 : P_1)$. Puisque $\Phi(1 : x_P) = (1 : x_{2P})$, on en déduit

$$h(2P) = h(1 : x_P) = h(\Phi(1, x_P)) = 4h(P) + \mathcal{O}(1).$$

□

Théorème 5.2.9. *(i)* $h(P) = h(-P)$;
(ii) $h(P+Q) + h(P-Q) = 2h(P) + 2h(Q) + \mathcal{O}(1)$.

Démonstration. La partie (i) est immédiate. Montrons (ii). On peut supposer $Q \neq \pm P$ (sinon l'énoncé est immédiat). D'après 2.2.6, on a :

$$x_{P+Q} + x_{P-Q} = \frac{2(x_P + x_Q)(a + x_P x_Q) + 4b}{(x_P + x_Q)^2 - 4x_P x_Q}$$
$$x_{P+Q} x_{P-Q} = \frac{(x_P x_Q - a)^2 - 4b(x_P + x_Q)}{(x_P + x_Q)^2 - 4x_P x_Q}.$$

En combinant le théorème 5.2.7(ii) et le lemme 5.2.10 ci-dessous on déduit que pour l'application

$$\Phi(T, U, V) : \mathbb{P}^2 \to \mathbb{P}^2$$
$$(T : U : V) \mapsto (U^2 - 4TV : 2U(aT + V) + 4bT^2 : (aT - V)^2 - 4bTU)$$

on a

$$h(\Phi(x)) = 2h(x) + \mathcal{O}(1).$$

Soient

$$\psi : (E \setminus 0_E)^2 \to \mathbb{P}^2$$
$$(P, Q) \mapsto (1 : x_P + x_Q, x_P x_Q)$$

et $\mu(P, Q) = (P + Q, P - Q)$. On a alors $\psi \circ \mu = \Phi \circ \psi$ et, d'après le lemme 5.2.11 ci-dessous

$$h(\psi(P, Q)) = h(x_P) + h(x_Q) + \mathcal{O}(1).$$

On en déduit

$$\begin{aligned} h(P + Q) + h(P - Q) &= h(1 : x_{P+Q} + x_{P-Q} : x_{P+Q} x_{P-Q}) + \mathcal{O}(1) = \\ &= h(\psi \circ \mu(P, Q)) + \mathcal{O}(1) = H(\Phi \circ \psi(P, Q)) + \mathcal{O}(1) = \\ &= 2h(\psi(P, Q)) + \mathcal{O}(1) = 2h(P) + 2h(Q) + \mathcal{O}(1). \end{aligned}$$

□

Lemme 5.2.10. *Soit k un corps. Soient $a, b \in k^*$ avec $4a^3 + 27b^2 \neq 0$.*

(i) Les polynômes $x^3 + ax + b$ et $x^4 + 2ax^2 - 8bx + a^2$ dans $k[x]$ sont premiers entre eux.

(ii) Les polynômes homogènes $U^2 - 4TV, 2U(aT + V) + 4bT^2, (aT - V)^2 - 4bTU$ n'ont pas de zéro commun dans $\mathbb{P}^2_k$.

Démonstration. L'énoncé (i) résulte de l'égalité :

$$\begin{aligned} (3x^2 + 4a)(x^4 - 2ax^2 - 8bx + a^2) - (3x^3 - 5ax - 27b)(x^3 + ax + b) = \\ = 4a^3 + 27b^2. \quad (5.8) \end{aligned}$$

L'énoncé (ii) est évident si $T = 0$. Supposons $T \neq 0$ et notons $u = U/2T$ et $v = V/T$. On a $u^2 - v = 2u(a + v) + 4b = 0$ et $(v - a)^2 - 8bu = 0$, d'où $u^4 - 2au^2 - 8bu + a^2 = u^3 + au + b$, contradiction avec (5.8). □

Lemme 5.2.11. *Soient $\alpha, \beta \in \overline{\mathbb{Q}}$. Alors*

$$1/2H(\alpha)H(\beta) \leq H(1 : \alpha + \beta : \alpha\beta) \leq 2H(\alpha)H(\beta).$$

Démonstration. Soit K un corps de nombres, tel que $\alpha, \beta \in K$. L'énoncé résulte des deux observations suivantes :

$$\max\{1, |\alpha + \beta|_v, |\alpha\beta|_v\} = \max\{1, |\alpha|_v\}\max\{1, |\beta|_v\}, v \in \Sigma_{fini}(K);$$

$$1/2 \max\{1, |\alpha|_v\}\max\{1, |\beta|_v\} \leq \max\{1, |\alpha + \beta|_v, |\alpha\beta|_v\} \leq \\ \leq 2\max\{1, |\alpha|_v\}\max\{1, |\beta|_v\}, v \in \Sigma_\infty(K).$$

□

5.2.3 Hauteur de Néron-Tate sur une courbe elliptique

Le but de cette section est de définir une fonction hauteur sur les points d'une courbe elliptique E qui soit une forme quadratique.

Lemme 5.2.12. *Soit S un ensemble. Supposons qu'on a des fonctions $h : S \to \mathbb{R}$ et $g : S \to S$ telles qu'il existe des constantes $d > 1$ et $c > 0$ telles que*

$$|h(g(x)) - dh(x)| < c \text{ pour tout } x \in S.$$

Alors pour tout $x \in S$ la suite $x_n = \frac{h(g^n(x))}{d^n}$ converge dans $\mathbb{R}$. Si $\hat{h}(x)$ est la limite de la suite (x_n), alors

$$|h(x) - \hat{h}(x)| \leq c/(d-1)$$
$$\hat{h}(g(x)) = d\hat{h}(x).$$

Démonstration. Montrons que la suite (x_n) est une suite de Cauchy. On écrit l'inégalité $|h(g(x)) - dh(x)| < c$ pour $x = g^{k-1}(x)$:

$$-\frac{c}{d^k} \leq \frac{h(g^k(x))}{d^k} - \frac{h(g^{k-1}(x))}{d^{k-1}} \leq \frac{c}{d^k}.$$

On prend la somme de ces inégalités entre $n+1$ et $n+m$ et on obtient

$$-\frac{c}{d^n(d-1)} \leq \frac{h(g^{n+m}(x))}{d^{n+m}} - \frac{h(g^n(x))}{d^n} \leq \frac{c}{d^n(d-1)}.$$

La suite (x_n) est donc une suite de Cauchy, on note $\hat{h}(x)$ sa limite. En passant à la limite dans les inégalités ci-dessus on obtient

$$-\frac{c}{d^n(d-1)} \leq \hat{h}(x) - \frac{h(g^n(x))}{d^n} \leq \frac{c}{d^n(d-1)},$$

d'où $|h(x) - \hat{h}(x)| \leq c/(d-1)$. De plus,

$$\hat{h}(g(x)) = \lim_{n\to\infty} h(g^{n+1}(x))/d^n = d \lim_{n\to\infty} h(g^{n+1}(x))/d^{n+1} = d\hat{h}(x).$$

□

Soit E une courbe elliptique définie sur un corps de nombres K. D'après le théorème 5.2.8, si l'on pose $S = E(K)$, h la hauteur de Weil sur E et g la multiplication par 2 sur $E(K)$, alors les condition du lemme précédent sont vérifiées (avec $d = 4$). On peut donc faire la définition suivante :

Définition 5.2.13. La hauteur de **Néron-Tate** sur E est définie par

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(x_{2^n P})}{4^n}.$$

Théorème 5.2.14. *(i)* $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$;
(ii) $\hat{h}(P) = 0$ *si et seulement si* P *est un point de torsion.*

Démonstration. L'énoncé (i) s'obtient en passant à la limite quand n tend vers ∞ dans les inégalités

$$-c/4^n \leq \frac{h(2^n(P+Q))}{4^n} + \frac{h(2^n(P-Q))}{4^n} - \frac{h(2^n P)}{4^n} - \frac{h(2^n Q)}{4^n} \leq c/4^n$$

du théorème 5.2.9.

Si $mP = 0$, alors $0 = \hat{h}(mP) = m^2\hat{h}(P)$, d'où $\hat{h}(P) = 0$. Inversement, si $\hat{h}(P) = 0$, alors $\hat{h}(mP) = 0$ pour tout m. On a donc que l'ensemble $\{mP, m \in \mathbb{Z}\}$ est de hauteur bornée, il est donc fini et on déduit que le point P est de torsion. □

On obtient comme corollaire :

Corollaire 5.2.15. *Soit E une courbe elliptique définie sur un corps de nombres K. Alors le sous-groupe de torsion $E(K)_{tors}$ de $E(K)$ est un groupe fini.*

Démonstration. L'énoncé résulte du théorème précédent et le fait qu'on n'a qu'un nombre fini de points de hauteur bornée. □

5.3 Théorème de Mordell-Weil

Le but de cette section est de démontrer le théorème célèbre suivant qui donne la structure du groupe des points rationnels d'une courbe elliptique sur un corps de nombres :

Théorème 5.3.1. [Mordell-Weil] *Soit E une courbe elliptique définie sur un corps de nombres K. Le groupe $E(K)$ est un groupe abélien de type fini.*

En particulier $E(K) = E(K)_{tors} \oplus \mathbb{Z}^r$ où le groupe des points de torsion $E(K)_{tors}$ de E est fini et r est par définition le **rang** de E.

La démonstration se fait en deux étapes :

1. Soit E/K une courbe elliptique définie par une equation $y^2 = x^3 + ax + b$ telle que le polynôme $P_3(x) = x^3 + ax + b$ admet trois racines dans K. Un argument de descente et l'existence de la hauteur $\hat{h}$ sur $E(K)$ (qui est quadratique) montre que le théorème 5.3.1 découle de sa version "faible" : le groupe $E(K)/2E(K)$ est fini.
2. Pour démontrer le théorème de Mordell-Weil "faible" on construit un homomorphisme $E(K) \to (K^*/K^{*2})^3$ dont le noyau est égal à $2E(K)$ et l'image est finie. Cette dernière propriété utilise en particulier le théorème des unités de Dirichlet dans les anneaux des entiers d'un corps de nombres (voir ci-dessous).

5.3.1 Descente

Proposition 5.3.2. *Soit G un groupe abélien et soit $q : G \to \mathbb{R}$ une forme quadratique. Supposons*

(i) le quotient $G/2G$ est fini ;

(ii) pour tout $c \in \mathbb{R}$, l'ensemble $\{x \in G, q(x) \leq c\}$ est fini.

Alors le groupe G est un groupe abélien de type fini : si S est l'ensemble des représentants pour chaque classe dans $G/2G$ et si $c = max_{x \in S} q(x)$, alors l'ensemble $\{x \in G\, q(x) \leq c\}$ engendre G.

Démonstration. Notons d'abord que pour tout $x \in G$ on a $q(x) \geq 0$. En effet, si cela n'était pas le cas, on aurait $q(mx) = m^2 q(x) < 0$ pour tout entier $m > 0$, ce qui contredit *(ii)*. On peut donc définir

$$|x| = \sqrt{q(x)}.$$

Comme q est une forme quadratique, on a $|mx| = m|x|$ pour tout $m > 0$ et $|x+y| \leq |x| + |y|$.

Soit c comme dans l'énoncé et soit $x \in G$ avec $q(x) > c$. On peut écrire $x = y_1 + 2x_1$ pour $x_1 \in G$ et y_1 dans l'ensemble des représentants de $G/2G$, en particulier $|y_1| \leq \sqrt{c}$. On a

$$|x_1| = \frac{1}{2}|x_0 - y_1| \leq \frac{1}{2}|x_0| + |y_1| \leq \frac{1}{2}(|x_0| + \sqrt{c}) < |x_0|.$$

On construit alors par récurrence une suite (x_n) avec $x_0 = x$ et $x_n = y_{n+1} + 2x_{n+1}$ et $|x_{n+1}| < |x_n|$. D'après la condition de finitude (ii), il existe n_0 tel que $|x_{n_0|} < \sqrt{c}$. On obtient donc que x est une combinaison de y_i et x_i, $i \leq n_0$ qui sont dans l'ensemble fini S. □

Version "faible" implique le théorème 5.3.1. Soit E/K une courbe elliptique définie par une équation $y^2 = x^3 + ax + b$. Soit L/K une extension finie telle que L contient le corps de décomposition du polynôme $P(x) = x^3 + ax + b$. On a une inclusion évidente $E(K) \subset E(L)$. Ainsi, si $E(L)$ est un groupe de type fini, alors $E(K)$ l'est aussi (cf. les exemples après la proposition 1.1.10, appliqués aux $\mathbb{Z}$-modules $E(K)$ et $E(L)$). Quitte à changer K par L, on peut donc supposer que E est donné par une équation (5.9).

La version "faible" donne la finitude du groupe $E(K)/2E(K)$. Par ailleurs, on dispose de la hauteur de Néron-Tate $\hat{h} : E(K) \to \mathbb{R}$ qui est une forme quadratique (voir les exercices) et qui vérifie la condition que pour tout $c \in \mathbb{R}$, l'ensemble $\{x \in E(K), \hat{h}(x) \leq c\}$ est fini. D'après la proposition 5.3.2, le groupe $E(K)$ est un groupe abélien de type fini. □

5.3.2 Théorème des unités de Dirichlet

Pour démontrer le théorème de Mordell-Weil nous aurons bésoin de résultats supplémentaires sur les unités dans $\mathcal{O}_K$.

Définition 5.3.3. Soit S un ensemble fini d'idéaux premiers dans $\mathcal{O}_K$. L'anneau des **S-entiers algébriques** de K est l'anneau

$$\mathcal{O}_{K,S} = \{x \in K, \, \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \, \forall \mathfrak{p} \notin S\}.$$

On note $\mathcal{O}_{K,S}^*$ l'ensemble des **S-unités**. Notons que si S est vide, alors $\mathcal{O}_{K,S}^* = \mathcal{O}_K^*$.

Supposons que K a r_1 plongements réels et r_2 paires de plongements complexes conjugués. On considère un morphisme

$$\Phi_{K,S} : \mathcal{O}_{K,S}^* \to \mathbb{R}^{r_1+r_2+|S|}$$
$$\Phi_{K,S}(x) = \prod_{i=1,\ldots,r_1+r_2} \log \sigma_i(x) \cdot \prod_{v \in S} \log |x|_v.$$

Lemme 5.3.4. *L'image $\Phi_{K,S}(\mathcal{O}_{K,S}^*)$ est un sous-groupe discret de $\mathbb{R}^{r_1+r_2+|S|}$.*

Démonstration. Puisque Φ est un homomorphisme, l'image $I = \Phi_{K,S}(\mathcal{O}_{K,S}^*)$ est un sous-groupe de $V = \mathbb{R}^{r_1+r_2+|S|}$. Il suffit donc de montrer qu'il existe un voisinage T de $0 \in V$ tel que $T \cap I$ est fini. Soit

$$T = \{x = (x_1, \ldots x_{r_1+r_2+|S|}) \in V, \, |x_i| < 1, i \leq r_1+r_2, |x_j| < \log N\mathfrak{p}, j \text{ correspond à } \mathfrak{p} \in S.\}$$

Soit $x = \Phi_{K,S}(\alpha) \in T \cap I$. La condition $|x_j| < \log N\mathfrak{p}$ pour j correspondant à un premier $\mathfrak{p}$ implique que $|\mathrm{ord}_{\mathfrak{p}}(\alpha)| < 1$, d'où $|\mathrm{ord}_{\mathfrak{p}}(\alpha)| = 0$. Ainsi, $\alpha \in \mathcal{O}_K^*$. De plus,

$|\sigma_i(\alpha)|$ sont bornés pour tout $i = 1, \dots r_1 + r_2$. La finitude de $T \cap I$ résulte alors du lemme ci-dessous. □

Lemme 5.3.5. *Soit K un corps de nombres qui a r_1 plongements réels $\sigma_1, \dots \sigma_{r_1}$ et r_2 paires de plongements complexes conjugués $\sigma_{r_1+1}, \bar{\sigma}_{r_1+1}, \dots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+r_2}$. Soient $a_1, i = 1 \dots, r_1 + r_2$ des réels strictement positifs. Soit*

$$U = \{\alpha \in \mathcal{O}_K, |\sigma_i(\alpha)| \leq a_i \ \forall\, i\}.$$

Alors

(i) l'ensemble U est fini ;

(ii) si $(a_1, \dots, a_n) = (1, \dots, 1)$, alors tout $\alpha \in U$ est une racine de l'unité.

Démonstration. Soit $\alpha \in U$ et soit

$$\chi_{\alpha,K}(x) = \prod_{i=1}^{r_1}(x - \sigma_i(\alpha)) \prod_{j=1}^{r_2}(x - \sigma_{r_1+j}(\alpha))(x - \bar{\sigma}_{r_1+j}(\alpha)).$$

On a $\chi_{\alpha,K} \in \mathbb{Z}[x]$ (cf. les rappels après la définition 5.1.2). On a $\chi_{\alpha,K}(\alpha) = 0$. Puisque $|\sigma_i(\alpha)| \leq a_i \ \forall\, i$, les coefficients de $\chi_{\alpha,K}$ sont bornés. On n'a donc qu'un nombre fini de tels polynômes, d'où la finitude de U. Si $(a_1, \dots, a_n) = (1, \dots, 1)$, alors la condition $\alpha \in U$ implique que $\alpha^m \in U$ pour tout $m > 0$. Comme U est fini, on en déduit que α est une racine de l'unité. □

Théorème 5.3.6. [Dirichlet-Chevalley-Hasse] *Soit K un corps de nombres avec r_1 plongements réels et r_2 paires de plongements complexes conjugués. Soit S un ensemble fini d'idéaux premiers dans $\mathcal{O}_K$ de cardinal $|S|$ (éventuellement vide). Alors :*

(i) le groupe des S-unités $\mathcal{O}_{K,S}^*$ est un groupe de type fini ;

(ii) le rang du groupe $\mathcal{O}_{K,S}^*$ est égal à $r_1 + r_2 - 1 + |S|$.

Démonstration. On montre ici la partie (i) de ce théorème, cela nous suffit pour des applications à l'étude des courbes elliptiques.

D'après le lemme 5.3.5, $I := \Phi_{K,S}(\mathcal{O}_{K,S}^*)$ est un sous-groupe discret de $\mathbb{R}^{r_1+r_2+|S|}$. D'après le lemme ci-dessous, il existe des éléments $v_1, \dots v_m \in I$ tels que

(i) $v_i = \Phi_{K,S}(u_i)$, avec $u_i \in \mathcal{O}_{K,S}^*$;

(ii) pour tout élément $u \in \mathcal{O}_{K,S}^*$ on a $u = e \prod_i u_i^{r_i}$ avec $r_i \in \mathbb{Z}$ et $e \in \ker \Phi_{K,S}$.

Un élément $e \in \ker \Phi_{K,S}$ vérifie

(*) $\mathrm{ord}_{\mathfrak{p}}(e) = 0$ pour tout $\mathfrak{p} \in S$, en particulier, $e \in \mathcal{O}_K$;

(**) $|\sigma_i(e)| = 1$ pour tout i.

En particulier, les conditions du lemme 5.3.5(ii) sont satisfaites, on obtient donc que e est une racine de l'unité et l'ensemble des tels e est fini. On déduit de (ii) ci-dessus que le groupe $\mathcal{O}_{K,S}^*$ est un groupe de type fini.

□

Lemme 5.3.7. *Soit V un $\mathbb{R}$-espace vectoriel de dimension finie. Soit $I \subset V$ un sous-groupe discret. Alors il existe des vecteurs $v_1, \ldots, v_m \in V$ qui sont $\mathbb{R}$-linéairement indépendants et tels que*

$$I = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m.$$

Démonstration. On prend $w_1, \ldots, w_n$ un ensemble maximal d'éléments de I qui sont indépendants sur $\mathbb{R}$. Ainsi $I' = \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n \subset I$ et tout élément $a \in I$ s'écrit comme $a = r_1w_1 + \ldots + r_nw_n$ avec $r_i \in \mathbb{R}$. Soit

$$T = \{\sum \lambda_i w_i, 0 \leq \lambda_i \leq 1.\}$$

Puisque I est discret, $T \cap I$ est fini : $T \cap I = \{a_1, \ldots, a_s\}$. D'après ce qui précède, tout $a \in I$ s'écrit comme $a = a_i + a'$ avec $a' \in I'$. En particulier, I' est un sous-groupe d'indice fini dans I, i.e. $dI \subset I'$ pour d entier. On a donc que $I \subset \frac{1}{d}I'$ et $\frac{1}{d}I'$ est un $\mathbb{Z}$-module libre de type fini de rang n. Ainsi I est un $\mathbb{Z}$-module libre de type fini de rang $n \leq m$: soient $v_1, \ldots v_m$ les générateurs de I. Comme $w_1, \ldots, w_n$ sont indépendants sur $\mathbb{R}$ et $\sum_{i=1}^{n} \mathbb{R}w_i \subset \sum_{j=1}^{r} \mathbb{R}v_j$, on en déduit que $n = m$ et que $v_1, \ldots, v_m$ sont $\mathbb{R}$-linéairement indépendants. □

5.3.3 Théorème de Mordell-Weil "faible"

Soit E une courbe elliptique définie sur un corps de nombres K par une équation

$$y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \tag{5.9}$$

On définit une application $\phi = (\phi_1, \phi_2, \phi_3) : E(K) \to (K^*/K^{*2})^3$ par

$$\phi_i(P) = \begin{cases} x_P - \alpha_i & P \neq P_i, 0_E \\ (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}), & P = P_i \\ 1 & P = 0_E \end{cases}$$

où l'on écrit $P = (x_P, y_P)$ les coordonnées du point P ; les indices $i-1$ et $i+1$ sont modulo 3.

Proposition 5.3.8. *L'application ϕ est un homomorphisme.*

Démonstration. D'après la définition, pour tout point $P \in E(K)$, on a

$$\phi(P) = \phi(-P) = \phi(P)^{-1} \tag{5.10}$$

dans $(K^*/K^{*2})^3$. Soient $P, Q \in E(K)$ et soit $R = -(P + Q)$, i.e.

$$P + Q + R = 0_E.$$

On a donc $\phi(P+Q) = \phi(R)$ et il s'agit de montrer que

$$\phi_i(P)\phi_i(Q)\phi_i(R) = 1, i = 1, 2, 3. \tag{5.11}$$

Soit $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$. Soit $y = \lambda x + \mu$ l'équation de la droite L qui coupe E en trois points P, Q, R, i.e. l'équation

$$f(x) - (\lambda x + \mu)^2 = 0$$

admet trois racines x_P, x_Q, x_R. On a les cas suivants à considérer :

1. P, Q, R sont tous distincts de P_i et de 0_E. On pose $x = x' + \alpha_i$ dans l'équation ci-dessus :
$$g(x) := f(x' + \alpha_i) - (\lambda x' + \lambda\alpha_i + \mu)^2 = 0$$
admet trois racines $x_P - \alpha_i, x_Q - \alpha_i, x_R - \alpha_i$. Comme $f(\alpha_i) = 0$, le coefficient constant du polynôme $g(x)$ est $(\lambda\alpha_i + \mu)^2$. On a donc
$$(x_P - \alpha_i)(x_Q - \alpha_i)(x_R - \alpha_i) = (\lambda\alpha_i + \mu)^2,$$
ce qui montre bien (5.11) dans ce cas.
2. Un des points P, Q, R est le point 0_E. D'après (5.10), on peut supposer que $R = 0_E$. On obtient alors (5.11) en appliquant encore une fois (5.10).
3. Un des points P, Q, R est le point P_i. On peut supposer $i = 1$ pour simplifier les notations. D'après (5.10), on peut supposer que $R = P_1$. On procède comme dans le premier cas : l'équation de la droite L est $y = \lambda(x - \alpha_1)$ et l'équation
$$f(x) = \lambda^2(x - \alpha_1)^2$$
admet trois racines : x_P, x_Q et α_1, i.e. l'équation
$$(x - \alpha_2)(x - \alpha_3) = \lambda^2(x - \alpha_1)$$
admet deux racines x_P et x_Q. Soit $x = x' + \alpha_1$. On a donc que l'équation
$$(x' + (\alpha_1 - \alpha_2))(x' + (\alpha_1 - \alpha_3)) = \lambda^2(x')^2$$
admet deux racines $\phi_1(P)$ et $\phi_1(Q)$, d'où $\phi_1(P)\phi_1(Q) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) = \phi_1(R)$, ce qui implique (5.11).

□

Proposition 5.3.9. *Le noyau de l'application ϕ est $2E(K)$.*

Démonstration. D'après la proposition précédente $\phi(2P) = \phi(P+P) = (\phi(P))^2 = 1$, donc $2E(K) \subset \ker\phi$. Il suffit de montrer l'inclusion $\ker\phi \subset 2E(K)$. Soit $P \in \ker\phi$. On peut donc trouver $z_i \in K^*$, $i = 1, 2, 3$ tels que

$$x_P - \alpha_i = z_i^2. \tag{5.12}$$

Soient u, v, w tels que

$$u + v\alpha_i + w\alpha_i^2 = z_i$$

(en effet, u, v, w sont des solutions d'un système linéaire de type Vandermonde.) Les équations (5.12) donnent des conditions suivants :

$$\begin{cases} u^2 - 2vwb - x = 0 \\ 2uv - 2vwa - bw^2 + 1 = 0 \\ v^2 + 2uw - aw^2 = 0, \end{cases}$$

d'où $v^3 + vw^2a + bw^3 - w = 0$. Notons que $w \neq 0$ (sinon $v = 0$ et on obtient une contradiction $1 = 0$ de la deuxième équation). On a donc

$$(v/w)^3 + a(v/w) + b = (1/w)^2.$$

On a donc que $Q = (v/w, 1/w)$ est un point de $E(K)$. On vérifie que $P = 2Q$:

$$\begin{aligned} x_{2Q} = \frac{(v/w)^4 - 2a(v/w)^2 - 8b(v/w) + a^2}{4((v/w)^3 + a(v/w) + b)} = \\ = \frac{v^4 - 2av^2w^2 - 8bvw^3 + a^2w^4}{4w^2} = \\ = \frac{(aw^2 - 2uw)^2}{4w^2} + \frac{1}{4}(-2av^2 - 8bvw + aw^2) = \\ = u^2 - 2vwb - \frac{a}{2}(v^2 - aw^2 + 2uw) = x. \quad (5.13) \end{aligned}$$

□

Proposition 5.3.10. *L'image $\phi(E(K))$ de l'application ϕ dans $(K^*/K^{*2})^3$ est finie.*

Démonstration. D'après le théorème 5.1.5, le groupe des classes $Cl(\mathcal{O}_K)$ est fini. On peut donc trouver un ensemble fini S de places de K tel que $\mathcal{O}_{K,S}$ est un anneau principal. Quitte à agrandir S, on peut de plus supposer que $\Delta_E = -(4a^3 + 27b^3)$ est dans $\mathcal{O}_{K,S}^*$. On a

$$\Delta_E = ((\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3))^2,$$

d'où $\alpha_i - \alpha_j \in \mathcal{O}_{K,S}^*$. Soit $P \in E(K)$. On écrit $x_P = u/v$ et $y_P = w/t$ avec $u, v, w, t \in \mathcal{O}_{K,S}$ et

$$(u, v) = (w, t) = 1 \text{ dans } \mathcal{O}_{K,S}. \quad (5.14)$$

On a

$$w^2v^3 = t^2(u - v\alpha_1)(u - v\alpha_2)(u - v\alpha_3).$$

En utilisant les conditions (5.14), on en déduit que $v^3 = t^2$, quitte à multiplier v et t par des unités. On peut donc écrire $v = s^2$ et $t = s^3$, d'où

$$P = (u/s^2, w/s^3),\ w^2 = (u - \alpha_1 s^2)(u - \alpha_2 s^2)(u - \alpha_3 s^2).$$

Tout diviseur commun de $(u-\alpha_1 s^2)$ et $(u-\alpha_2 s^2)$ divise $(\alpha_1-\alpha_2)s^2$ et $(\alpha_1-\alpha_2)u$, et il divise donc $(\alpha_1-\alpha_2) \in \mathcal{O}_{K,S}^*$. On en déduit que $(u-\alpha_1 s^2)$, $(u-\alpha_2 s^2)$ et $(u-\alpha_3 s^2)$ sont deux à deux premiers entre eux, d'où

$$x_P - \alpha_i = \frac{u-\alpha_i s^2}{s^2} = \gamma_i r_i^2, \gamma_i \in \mathcal{O}_{K,S}^*.$$

Ainsi, $\phi(P) = (\gamma_1, \gamma_2, \gamma_3)$. Le théorème des unités de Dirichlet-Chevalley-Hasse 5.3.6 implique que le groupe $O_{K,S}^*/(O_{K,S}^*)^2$ est fini. On en déduit que $\phi(E(K))$ est fini. □

Théorème 5.3.11. [Mordell-Weil "faible"] *Soit E une courbe elliptique définie par une équation (5.9). Le groupe $E(K)/2E(K)$ est fini.*

Démonstration. D'après la proposition 5.3.9, $E(K)/2E(K) \simeq \phi(E(K))$. Ce dernier groupe est fini d'après la proposition 5.3.10. □

5.3.4 Calcul du groupe $E(\mathbb{Q})$.

Soit E une courbe elliptique définie sur $\mathbb{Q}$ par une équation

$$y^2 = x^3 + ax + b = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3).$$

La preuve du théorème de Mordell-Weil faible donne une méthode pour déterminer le groupe $E(\mathbb{Q})/2E(\mathbb{Q})$: on voit que $Im\,\phi \subset \{(\gamma_1,\gamma_2,\gamma_3) \in (\mathcal{O}_{K,S}^*/(\mathcal{O}_{K,S}^{*2}))^3, \gamma_1\gamma_2\gamma_3 = 1\}$ où $S = \{p \text{ premier}, p|\Delta_E\}$ (voir les exemples dans les exercices ci-dessous). Par ailleurs, pour déterminer le groupe $E(\mathbb{Q})_{tors}$ on utilise le théorème suivant dont la preuve peut être étudiée dans l'enseignement d'approfondissement :

Théorème 5.3.12 (Lutz-Nagell)**.** *Soit E une courbe elliptique $y^2 = x^3 + ax + b$ avec $a, b \in \mathbb{Z}$. Soit $P \in E(\mathbb{Q})$ un point de torsion. Alors $x_P, y_P \in \mathbb{Z}$ et soit $y_P = 0$, soit $y_P^2 | 4a^3 + 27b^2$.*

5.4 Exercices

1. Que vaut a) $H(\frac{2}{3})$; b) $H(\frac{1+\sqrt{-5}}{2})$?
2. Soient G un groupe abélien, $h : G \to R$ une fonction qui satisfait l'égalité du parallélogramme :

   $$h(P+Q) + h(P-Q) = 2h(P) + 2h(Q), \forall P, Q \in G.$$

   Le but de cet exercice est de montrer que h est une forme quadratique : $h(mP) = m^2 h(P) \forall P \in G, m \in \mathbb{Z}$ et $(P,Q) \mapsto \langle P, Q\rangle = h(P+Q) - h(P) - h(Q)$ est une forme bilinéaire symétrique.

   (a) Montrer que $h(-P) = h(P)$ et que $h(0) = 0$.

   (b) Montrer que $h(mP) = m^2 h(P) \forall P \in G, m \in \mathbb{Z}$.

(c) Montrer que $\langle P+R, Q\rangle = \langle P, Q\rangle + \langle R, Q\rangle$ (on pourra appliquer l'égalité de parallélogramme à $(P+R, Q)$, $(P, R-Q)$, $(P+Q, R)$ et (R, Q)).

(d) En déduire que h est une forme quadratique.

3. Soit E la courbe elliptique $y^2 = x^3 - x$. Determiner le groupe $E(\mathbb{Q})$.

4. Supposons que E est une courbe elliptique sur $\mathbb{Q}$ telle que $E(\mathbb{Q})$ est engendré par le point P d'ordre infini. Donner un exemple d'ensemble des représentants de $E(\mathbb{Q})/2E(\mathbb{Q})$ qui n'engendre pas $E(\mathbb{Q})$.

5. Soit E une courbe elliptique $y^2 = x^3+ax+b$ avec $a, b \in \mathbb{Z}$ et telle que le polynôme x^3+ax+b admette trois racines entières. Soit $s = \#\{p \mid p \text{ divise } 2\Delta_E\}$. Montrer que le rang r du groupe $E(\mathbb{Q})$ vérifie :

$$r \leq 2s - 1.$$

6. Soit $E : y^2 = x^3 - 25x$ une courbe elliptique sur $\mathbb{Q}$. Montrer que $(-4, 6) \in E(\mathbb{Q})$. Que peut-on dire sur le rang de E ?

7. Le but de cet exercice est de determiner le groupe $E(\mathbb{Q})$ pour la courbe elliptique $E : y^2 = x^3 - 4x$.

(a) Trouver tous les points de 2-torsion de E.

(b) Utiliser la méthode de la descente pour montrer que $\#Im\phi \leq 8$.

(c) Montrer que le triplet $(1, 2, 2)$ n'est pas dans l'image de ϕ.

(d) Determiner le groupe $E(\mathbb{Q})$.

Chapitre 6

Le point de vue complexe

Cette partie donne une brève description des propriétés des courbes elliptiques définies sur le corps $\mathbb{C}$. Dans ce cas, pour étudier les propriétés des courbes elliptiques on dispose de plus des méthodes analytiques.

6.1 Fonctions elliptiques

Soient $\omega_1, \omega_2 \in \mathbb{C}$ linéairement indépendants sur $\mathbb{R}$. Soit $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subset \mathbb{C}$ le réseau correspondant. Le **parallélogramme fondamental** de Λ est l'ensemble

$$\prod = \{t_1\omega_1 + t_2\omega_2, 0 \leq t_1, t_2 < 1\}.$$

On a une bijection

$$\prod \xrightarrow{\sim} \mathbb{C}/\Lambda \tag{6.1}$$

et on va donc identifier $\prod$ à $\mathbb{C}/\Lambda$.

Définition 6.1.1. Une **fonction Λ-elliptique** est une fonction méromorphe sur $\mathbb{C}$ telle que

$$f(z+w) = f(z)\, \forall w \in \Lambda, z \in \mathbb{C}.$$

Ces fonctions apparaissent dans l'étude des intégrales elliptiques

$$\int_\infty^x \frac{\mathrm{dt}}{\sqrt{t(t-1)(t-\lambda)}}.$$

Souvent on ne précise pas le réseau Λ et l'on dit «une fonction elliptique». On peut voir une fonction elliptique f comme une fonction sur le quotient $\mathbb{C}/\Lambda$, via l'isomorphisme (6.1) ci-dessus.

L'ensemble des fonctions Λ-elliptiques forme un corps, que l'on note $\mathcal{M}(\Lambda)$.

Rappelons que pour toute fonction méromorphe f et pour tout $z \in \mathbb{C}$, on définit l'ordre $ord_z f$ et le résidu $res_z f$. Si f est elliptique, on a que $ord_z f$ et $res_z f$ ne dépendent que de la classe de z dans $\mathbb{C}/\Lambda$. On a les propriétés suivantes (voir les exercices).

Proposition 6.1.2. *Soit f une fonction elliptique.*

1. *Si f n'a pas de pôles, alors f est constante ;*
2. $\sum_{z\in\mathbb{C}/\Lambda} res_z f = 0$;
3. $\sum_{z\in\mathbb{C}/\Lambda} ord_z f = 0$;
4. $\sum_{z\in\mathbb{C}/\Lambda} ord_z f \cdot z \in \Lambda$.
5. *si f a un seul pôle z_0, alors z_0 n'est pas un pôle simple.*

Les fonctions constantes sont évidemment elliptiques. On définit

$$\rho(z) = \frac{1}{z^2} + \sum_{w\in\Lambda\setminus\{0\}} (\frac{1}{(z-w)^2} - \frac{1}{w^2})$$

la **fonction de Weierstrass**.

Proposition 6.1.3.

1. *la fonction ρ et sa dérivée ρ' sont des fonctions elliptiques ;*
2. *le corps $\mathcal{M}(\Lambda)$ des fonctions elliptiques est engendré par ρ et ρ' :*

$$\mathcal{M}(\Lambda) = \mathbb{C}(\rho, \rho');$$

3. *on a*

$$\rho'(z)^2 = 4\rho(z)^3 - 60G_4\rho(z) - 140G_6 \tag{6.2}$$

où $G_{2k} = G_{2k}(\Lambda) = \sum_{w\in\Lambda\setminus\{0\}} \frac{1}{w^{2k}}, k \geq 2$;

4. *pour*

$$g_2 = 60G_4 \text{ et } g_3 = 140G_6 \tag{6.3}$$

on a $g_2^3 - 27g_3^2 \neq 0$.

On vérifie également les formules de l'addition pour la fonction de Weierstrass :

$$\rho(z_1 + z_2) = -\rho(z_1) - \rho(z_2) + \frac{1}{4}(\frac{\rho'(z_1) - \rho'(z_2)}{\rho(z_1) - \rho(z_2)})^2 \tag{6.4}$$

$$\rho(2z) = -2\rho(z) + \frac{1}{4}(\frac{\rho''(z)}{\rho'(z)})^2. \tag{6.5}$$

6.2 Propriétés des courbes elliptiques sur $\mathbb{C}$

6.2.1 Le groupe des points

Proposition 6.2.1. *Soit E une courbe elliptique complexe définie par une équation*

$$Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$$

où g_2 et g_3 sont définis dans (6.3). On a alors une application biholomorphe

$$\Psi : \mathbb{C}/\Lambda \to E,\ z \mapsto [\rho(z) : \rho'(z) : 1]$$

qui est un isomorphisme de groupes.

Démonstration. Montrons d'abord la surjectivité. Soit $(x, y) \in E$. On a alors que la fonction $h(z) = \rho(z) - x$ a un (double) pôle en 0. Ainsi h admet aussi un zéro z_0 dans $\prod$. On déduit de 6.2 que $\rho'(z_0)$ ou $\rho'(-z_0)$ vaut y. Ainsi, soit z_0, soit $-z_0$ convient.

Pour montrer l'injectivité on suppose que $\rho(z_1) = \rho(z_2)$ et que $\rho'(z_1) = \rho'(z_2)$. Le but est de montrer que $z_1 - z_2 \in \Lambda$. On distingue des cas suivants :

1. Si z_1 est le pôle de ρ, alors z_2 l'est aussi, d'où $z_1 - z_2 \in \Lambda$.
2. Supposons que z_1 n'est pas un pôle de ρ. Notons que pour ω_1, ω_2 et $\omega_3 = \omega_1 + \omega_2$ on a $\rho'(\omega_i/2) = \rho'(-\omega_i/2) = -\rho'(\omega_i/2)$ (la première égalité résulte du fait que ρ' est elliptique). On a donc que ρ' a trois zéros $\omega_i/2$ dans $\prod$. Comme ρ' n'a qu'un seul pôle d'ordre 3 dans $\prod$, on a que ρ' n'a pas d'autres zéros dans $\prod$.

   Si maintenant $z_1 \neq \omega_i/2$ on introduit $h(z) = \rho(z) - \rho(z_1)$. Alors $h(z) = 0$ pour $z = z_1, z_2$ ou $-z_1$. Comme h n'a qu'un seul pôle (double) dans $\prod$, on déduit que $z_2 = -z_1$. Alors $y = \rho'(z_2) = \rho'(-z_1) = -y$ d'où $\rho'(z_1) = 0$ ce qui n'est pas possible d'après ce qui précède.
3. Si $z_1 = \omega_i/2$, on trouve $\rho'(z_1) = 0$, i.e. z_1 est une racine double de h. Mais h n'a que deux zéros (et $h(z_2) = 0$), d'où $z_1 = z_2$.

Pour montrer que Ψ est un homomorphisme de groupes, on utilise les formules de l'addition pour la fonction de Weierstrass, on le laisse en exercice. □

Remarque 6.2.2.

1. Soient $a, b \in \mathbb{C}$ tels que $a^3 - 27b^2 \neq 0$. Le théorème d'uniformization dit qu'il existe un unique réseau $\Lambda \subset \mathbb{C}$ tel que $g_2(\Lambda) = a$, $g_3(\Lambda) = b$. Quitte à faire un changement linéaire en coordonnées, toute courbe elliptique complexe est donnée par une équation $y^2 = 4x^3 - g_2x - g_3$ avec $g_2^3 - 27g_3^2 \neq 0$. On peut donc toujours identifier une courbe elliptique complexe avec un quotient $\mathbb{C}/\Lambda$ pour Λ un réseau convenable. On appelle un tel quotient un **tore complexe**.
2. Comme une conséquence directe de la proposition 6.2.1, on obtient la structure du sous-groupe $E[n]$ des points de n-torsion, pour une courbe E définie

sur le corps $\mathbb{C}$. En effet, le noyau de la multiplication par n sur $\mathbb{C}/\Lambda$ s'identifie à $\{z \in \mathbb{C}, nz \in \Lambda\}/\Lambda = (\mathbb{Z}/n)^2$.

On dispose aussi d'une autre interprétation du groupe des points d'une courbe elliptique complexe, en tant qu'un groupe des diviseurs.

Définition 6.2.3. Un **diviseur** D sur $\mathbb{C}/\Lambda$ est une somme finie formelle

$$D = \sum n_i z_i,\ z_i \in \mathbb{C}/\Lambda.$$

On définit le **degré** de D par $deg(D) = \sum n_i$. Un diviseur **principal** est un diviseur D de la forme

$$D = \sum_{z \in \mathbb{C}/\Lambda} (ord_z f)z$$

où f est une fonction elliptique.

L'ensemble de tous les diviseurs sur $\mathbb{C}/\Lambda$ forme un groupe abélien. On note $Div(\mathbb{C}/\Lambda)$ ce groupe, $Div^0(\mathbb{C}/\Lambda)$ le sous-groupe des diviseurs de degré zéro et $Div^p(\mathbb{C}/\Lambda)$ le sous-groupe des diviseurs principaux. D'après la proposition 6.1.2.3 ci-dessus, on a $Div^p(\mathbb{C}/\Lambda) \subset Div^0(\mathbb{C}/\Lambda)$.

Théorème 6.2.4 (Abel-Jacobi)**.** *L'application*

$$Div(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda,\ \sum n_i z_i \mapsto \sum n_i \cdot z_i$$

induit un isomorphisme de groupes

$$\phi : Div^0(\mathbb{C}/\Lambda)/Div^p(\mathbb{C}/\Lambda) \xrightarrow{\sim} \mathbb{C}/L.$$

Démonstration. (idée) D'après la proposition 6.1.2, l'application ϕ est bien définie. D'après la définition, c'est bien un morphisme de groupes. Puisque $\phi(z - 0) = z$ pour tout $z \in \mathbb{C}/\Lambda$, l'application ϕ est surjective. Pour démontrer l'injectivité, si D est un diviseur tel que $\phi(D) = 0$, on construit explicitement une fonction f telle que $D = div(f)$. □

Corollaire 6.2.5. *Soit E la courbe elliptique complexe $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$ où g_2 et g_3 sont définis dans (6.3). On a alors un isomorphisme de groupes*

$$Div^0(\mathbb{C}/\Lambda)/Div^p(\mathbb{C}/\Lambda) \to E.$$

Démonstration. On obtient l'isomorphisme de l'énoncé par composition de l'application ϕ et l'application de la proposition 6.2.1. □

6.2.2 Les endomorphismes

Soit E une courbe elliptique. D'après la remarque 6.2.2, on peut l'identifier avec un tore $\mathbb{C}/\Lambda$. Par ailleurs, pour tout $u \in \mathbb{C}^*$, la multiplication par u induit un isomorphisme entre $\mathbb{C}/\Lambda$ et $\mathbb{C}/u\Lambda$. Quitte à multiplier par un élément $u \in \mathbb{C}$ on peut donc toujours supposer que $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$ avec τ dans le demi-plan $\mathcal{H}$ de Poincaré (i.e. $Im\tau > 0$.)

Proposition 6.2.6. *Deux tores complexes $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)$ et $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau')$ sont isomorphes si et seulement s'il existe une matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ telle que $\tau' = \frac{a\tau+b}{c\tau+d}$.*

Démonstration. Soit $\phi : \mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau') \to \mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)$ un homomorphisme. On a alors que ϕ est induit par la multiplication par un élément $\alpha \in \mathbb{C}$ tel que $\alpha(\mathbb{Z} \oplus \mathbb{Z}\tau') \subset \mathbb{Z} \oplus \mathbb{Z}\tau$. On a donc $\alpha = c\tau + d$ et $\alpha\tau' = a\tau + b$ avec $a, b, c, d \in \mathbb{Z}$. Ainsi $\tau' = \frac{a\tau+b}{c\tau+d}$. Puisque ϕ est un isomorphisme, on a que la matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ est inversible et, puisque $Im(\tau') = det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) Im(\tau)/|c\tau + d|^2$ on obtient bien $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$. □

Corollaire 6.2.7. *Soit $E = \mathbb{C}/\Lambda$ une courbe elliptique, où $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$. Alors*

$$End(E) = \begin{cases} \mathbb{Z}, & [\mathbb{Q}(\tau) : \mathbb{Q}] > 2 \\ \mathbb{Z} + \mathbb{Z}A\tau, & [\mathbb{Q}(\tau) : \mathbb{Q}] = 2. \end{cases}$$

Dans le deuxième cas, l'entier A est le coefficient du polynôme minimal $A\tau^2+B\tau+C$ de τ. On dit alors que E a une **multiplication complexe**.

Démonstration. On a $End(E) = \{\alpha \in \mathbb{C}, \mid \alpha\Lambda \subset \Lambda\}$. D'après la proposition précédente on a que $\alpha = c\tau + d$ correspond à une matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ telle que $\tau = \frac{a\tau+b}{c\tau+d}$. On a donc $c\tau^2 + (d-a)\tau - b = 0$. Si $[\mathbb{Q}(\tau) : \mathbb{Q}] > 2$, on obtient $c = b = 0, a = d$, i.e. la multiplication par d. Si $[\mathbb{Q}(\tau) : \mathbb{Q}] > 2$ et $A\tau^2 + B\tau + C$ est le polynôme miniimal de τ, on trouve de plus $c = mA, d - a = mB, -b = mC$, d'où $\alpha = mA\tau + d$. □

6.3 Exercices

1. Soit f une fonction elliptique.
   (a) Montrer que si f n'a pas de pôles, alors f est constante (on pourrait utiliser le théorème de Liouville).
   (b) En utilisant la formule des résidus, montrer que
      i. $\sum_{z \in \mathbb{C}/\Lambda} res_z f = 0$;
      ii. $\sum_{z \in \mathbb{C}/\Lambda} ord_z f = 0$;
      iii. $\sum_{z \in \mathbb{C}/\Lambda} ord_z f \cdot z \in \Lambda$.

2. (a) Montrer que la série

$$\rho(z) = \frac{1}{z^2} + \sum_{w \in \Lambda \setminus \{0\}} (\frac{1}{(z-w)^2} - \frac{1}{w^2})$$

définit une fonction méromorphe λ-péridodique sur $\mathbb{C}$. Quels sont les pôles de cette fonction ?

(b) Pour tout entier $k \geq 2$ vérifier que la série $G_{2k}(\lambda) = \sum w \in \Lambda \setminus \{0\} \frac{1}{w^{2k}}$ est convergente.

(c) Calculer le développement en série de Laurent de $\rho(z)$ au voisinage de 0 en fonction des $G_{2k}(\lambda)$.

(d) Montrer que

$$\rho'(z)^2 = 4\rho(z)^3 - 60G_4(\lambda)\rho(z) - 140G_6(\lambda).$$

(e) Montrer que pour $g_2 = 60G_4$ et $g_3 = 140G_6$ on a $g_2^3 - 27g_3^2 \neq 0$.

6.4 Complément : dernier théorème de Fermat

Pour terminer ce cours on indique le rôle des courbes elliptiques dans la preuve du grand théorème de Fermat.

Soit E une courbe elliptique définie sur $\mathbb{Q}$. Par un changement de variables convenable, on peut supposer que E est donnée par une équation

$$y^2 = x^3 + Ax + B,\ A, B \in \mathbb{Z}. \tag{6.6}$$

Pour tout premier p, on dispose d'une courbe

$$E_p : y^2 = x^3 + A_p x + B_p$$

où $A_p \in \mathbb{Z}/p$ (resp. B_p) est la réduction de A (resp. de B) modulo p. Si $p \not| \Delta_E$, la courbe E_p est une courbe elliptique sur $\mathbb{F}_p$. On dit que E a **une réduction additive** en p si $A_p = B_p = 0$. Si ce n'est pas le cas pour aucun premier p, on dit que E a une **réduction semi-stable**.

Pour tout premier p et pour tout $r > 0$ on définit $a_{p^r} = p^r + 1 - \#E_p(\mathbb{F}_{p^r})$ si E_p est lisse. Si ce n'est pas le cas, on définit $a_{p^r} \in \{-1, 1, 0\}$ suivant le type de réduction. Si $n = \prod p_i^{r_i}$ est un entier, on définit $a_n = \prod a_{p_i^{r_i}}$. À la courbe elliptique E on associe alors une série :

$$f_E(\tau) = \sum_{n=1}^{\infty} a_n q^n, q = e^{2\pi i \tau},$$

qui converge pour tout $\tau \in \mathcal{H}$.

Théorème 6.4.1 (**Wiles, Breuil, Conrad, Diamond, Taylor**). **(Conjecture de Taniyama-Shimura-Weil)**
Soit E une courbe elliptique (6.6). Alors la courbe E est modulaire : il existe un entier N tel que pour tout $\tau \in \mathcal{H}$ on a

1. $f_E(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^2 f_E(\tau)$, $\forall \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, *où* $\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z}), c \equiv 0\,(mod\ N)\}$;
2. $f_E(-\frac{1}{N\tau}) = \pm N\tau^2 f_E(\tau)$.

En 1994, A. Wiles a établi le théorème ci-dessus pour E semi-stable.

Soit maintenant

$$x^n + y^n = z^n, n \geq 3.$$

Supposons que cette équation admet une solution non-triviale (a, b, c) avec $a, b, c \in \mathbb{Z}$. Il suffit de considérer le cas $n = \ell$ un premier impair. En 1986, Frey a introduit une courbe elliptique associée à une telle solution

$$E_{\text{Frey}} : y^2 = x(x - a^\ell)(x + b^\ell).$$

Théorème 6.4.2 (Ribert, 1986)**.** *La courbe E_{Frey} n'est pas modulaire.*

Ce théorème et le théorème d'A.Wiles impliquent qu'une solution (a, b, c) de l'équation de Fermat ne peut pas exister.