ACCQ 207 - Cryptographie

1 Courbes elliptiques

1.1 Définitions

Def. Une **courbe elliptique** sur un corps K est

- soit la donnée d'une courbe algébrique E projective lisse de genre 1 sur K et d'un point $O_E \in E(K)$,
- soit la donnée d'une équation "de Weierstrass" de la forme $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ qui définit une courbe plane où les coefficients $a_1, a_2, a_3, a_4, a_6 \in K$ sont choisis pour que E soit lisse. La courbe admet alors un unique point à l'infini, noté O_E.

Rem. Lorsque K est de caractéristique différente de 2 ou 3, on se ramène par changement de variable à une équation de la forme $y^2 = x^3 + ax + b$. La lissité équuivaut donc à ce que $x^3 + ax + b$ soit sans racine double, i.e $\Delta = 4a^3 + 27b^2 \neq 0$ dans K.

1.2 Loi de groupe

Lem. Soit $D \in \mathrm{Div}^0(E)$, alors $\exists! P \in E(K), D \sim (P) - (O_E)$.

On a donc une bijection $\begin{array}{ccc} E(K) & \xrightarrow{\sim} & Cl^0(E)_K \\ P & \mapsto & (P) - (O_E) \end{array}$ avec $Cl^0(E)_K$ le groupe des classes d'équivalence linéaire de diviseurs de degré 0 définis sur K.

Def. On munit $E(K)$ d'une loi de groupe $+$ en transportant la loi de $Cl^0(E)_K$ par cette bijection.

Prop. (i) L'élément neutre de $E(K)$ est O_E.

(ii) $\forall P, Q \in E(K)$, $P+Q$ dans $E(K)$ est l'unique point tel que $(P)-(O_E)+(Q)-(O_E) \sim (P+Q)-(O_E)$ dans $\mathrm{Div}^0(E)$, i.e. tel que $\exists f \in E(K), \mathrm{div}(f) = (P) + (Q) - (P+Q) - (O_E)$.

(iii) Soit $D = \sum_{P \in E(K)} n_P \cdot (P)$ un diviseur sur E. Alors D est principal si et seulement si $\deg(D) = \sum_P n_P = 0$ et $\sum_p n_P P = O_E$ dans $E(K)$.

(iv) En particulier $P + Q + R = O_E \iff (P) - (O_E) + (Q) - (O_E) + (R) - (O_E) \sim 0$ dans $\mathrm{Div}^0(E)$.

(v) $\forall P \in E(K)$, $-P \in E(K)$ est l'unique point tel que $\exists f, \mathrm{div}(f) = (P) + (-P) - 2(O_E)$.

Rem. On a $P + Q + R = O_E$ si et seulement si P, Q, R sont les trois points d'intersection de E et d'une droite.

Rem. Si P est un point de coordonnées affines (x_P, y_P) alors $-P$ a pour coordonnées $(x_P, -y_P)$.