le théorème de Mordell-Weil

K corps de nombres (i.e. une extension finie de $\mathbb{Q}$)

E courbe elliptique sur K

Théorème (Mordell-Weil)

Le groupe $E(K)$ est de type fini :

$$E(K) \cong \underbrace{E(K)_{tors}}_{\text{groupe fini}} \times \mathbb{Z}^r \qquad r = \text{rang} \in \mathbb{Z}_{\geq 0}$$

La preuve consiste en deux étapes indépendantes, dont la première est :

Théorème (Mordell-Weil « faible »)

Soit K un corps de nombres, E une courbe elliptique sur K et $m \geq 2$ un entier.

Alors $E(K)/mE(K)$ est un groupe fini.

→ On commence par réduire la preuve à la situation où $E[m] \subset E(K)$ par :

Lemme : Soit L/K une extension finie galoisienne. Si $E(L)/mE(L)$ est fini, alors $E(K)/mE(K)$ est fini.

Démonstration : Considérons la suite exacte suivante

$$0 \to \underbrace{\frac{E(K) \cap mE(L)}{mE(K)}}_{\Phi} \to E(K)/mE(K) \to E(L)/mE(L)$$

(flèche : induite par l'inclusion $E(K) \subset E(L)$)

Pour tout $P \in \Phi$, soit $Q_P \in E(L)$ tel que $[m]Q_P = P$. Définissons l'application

$$\lambda_P : Gal(L/K) \longrightarrow E[m]$$
$$\sigma \longmapsto \sigma(Q_P) - Q_P$$

(bien définie car

$$[m]\left(\sigma(Q_P) - Q_P\right) = \sigma([m]Q_P) - [m]Q_P$$
$$= \sigma(P) - P$$
$$= 0\ )$$

$\Rightarrow P \in E(K)$

Si $P, P' \in \Phi$ satisfont à $\lambda_P = \lambda_{P'}$, alors

$\sigma(Q_P - Q_{P'}) = Q_P - Q_{P'}$ pour $\sigma \in \mathrm{Gal}(L/K)$,

donc $Q_P - Q_{P'} \in E(K)$. On a alors :

$$P - P' = [m](Q_P - Q_{P'}) \in {}_mE(K),$$

donc $P = P'$ car éléments de Φ. On obtient une injection

$$\Phi \hookrightarrow \mathrm{Maps}(\mathrm{Gal}(L/K), E[m])$$
$$P \longmapsto \lambda_P$$

et comme l'ensemble à droite est fini, Φ est aussi fini. Par conséquent,

$$0 \to \underset{\text{fini}}{\Phi} \to \underset{\text{fini}}{E(K)/mE(K)} \to \underset{\text{fini}}{E(L)/mE(L)}$$

□

Hypothèse : $\boxed{E[m] \subset E(K)}$

Définition : L'accouplement de Kummer

$$k : E(K) \times \mathrm{Gal}(\bar{K}/K) \longrightarrow E[m]$$

est défini comme suit : pour $P \in E(K)$,

soit $Q \in E(\bar{K})$ tel que $[m]Q = P$. Alors

$$\boxed{k(P,\sigma) = \sigma(Q) - Q}$$

Proposition : L'accouplement de Kummer satisfait aux propriétés suivantes :

a) il est bien défini

b) il est bilinéaire

c) son noyau à gauche est $mE(K)$

d) son noyau à droite est $Gal(\bar{K}/L)$

où $L = K\left([m]^{-1}E(K)\right)$

L = composition de $K(Q)$ pour tout $Q \in E(\bar{K})$ avec $[m]Q \in E(K)$

$\Rightarrow$ accouplement parfait bilinéaire

$$\boxed{E(K)/mE(K) \times Gal(L/K) \longrightarrow E[m]}$$

$Gal(L/K)$ agit sur $Gal(\bar{K}/K)$

Démonstration : a) comme avant, prenons $[m]^{-1}E(K)$

$$[m]\,k(P,\sigma) = [m]\left(\sigma(Q) - Q\right)$$
$$= \sigma([m]Q) - [m]Q = 0$$

et donc $K(P,\sigma) \in E[m]$. Si on choisit un autre point Q pour le calculer, il est de la forme $\underline{Q+T}$ avec $T \in E[m]$, d'où :

$$\sigma(Q+T) - (Q+T) = \sigma(Q) + \sigma(T) - Q - T = \sigma(Q) - Q$$

car $\sigma(T) = T$ par l'hypothèse $E[m] \subset E(K)$.

b) $K(P+P', \sigma) = K(P,\sigma) + K(P',\sigma)$ is obvious. For the second equality,

$$\begin{aligned} K(P, \sigma\tau) &= \sigma\tau(Q) - Q \\ &= \sigma(\tau(Q) - Q) + \sigma(Q) - Q \\ &= \sigma(K(P,\tau)) + K(P,\sigma) \\ &= K(P,\tau) + K(P,\sigma) \end{aligned}$$

since we saw that $K(P,\tau) \in E[m] \subset E(K)$.

c) If $P \in mE(K)$, then $P = [m]Q$ with $Q \in E(K)$, hence $\sigma(Q) - Q = 0$. Conversely, if $K(P,\sigma) = 0$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$, then $\sigma(Q) = Q$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$, hence $Q \in E(K)$.

d) Si $\sigma \in Gal(\bar{K}/L)$, alors $K(P,\sigma) = 0$ car $Q \in E(L)$ par définition. Réciproquement, si $K(P,\sigma) = 0$ pour tout $P \in E(K)$, alors pour tout $Q \in E(\bar{K})$ avec $[m]Q \in E(K)$, on a $0 = K([m]Q, \sigma) = \sigma(Q) - Q$, c'est-à-dire σ fixe $L \Rightarrow \sigma \in Gal(\bar{K}/L)$ □

→ Il suffit donc de démontrer que l'extension L/K est finie.

Rappel : sur $\mathbb{Q}$, toute valeur absolue est équivalente à

- soit $|x|_\infty = \max(x, -x)$
- soit $|x|_p$ pour un nombre premier p

avec $\left|p^n \frac{a}{b}\right| = p^{-n}$ si $p \nmid ab$.

($|x|' = |x|^c$ pour $c > 0$ réel (même topologie))

Pour un corps de nombres K, soit M_K l'ensemble de toutes les valeurs absolues sur K dont la restriction à $\mathbb{Q}$ est comme ci-dessus on écrit : $\boxed{M_K = M_K^0 \cup M_K^\infty}$

Pour chaque $|\cdot|_v \in M_K^\circ$, soit K_v la complétion de K par rapport à la topologie définie par v et soit k_v le corps résiduel (c'est-à-dire le quotient de l'anneau $\mathcal{O}_v = \{x \in K_v \mid |x|_v \leq 1\}$ par l'idéal maximal $\{x \in K_v \mid |x|_v < 1\}$). L'exemple à garder en tête est $K = \mathbb{Q}$, $|\cdot|_v = |\cdot|_p$, $K_v = \mathbb{Q}_p$, $k_v = \mathbb{F}_p$.

Une équation de Weierstrass

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

avec $a_1, \dots, a_6 \in \mathcal{O}_v$ est dite minimale si $v(\Delta)$ est minimal.

↑ discriminant ($= -16(4A^3 + 27B^2)$ pour la forme standard $y^2 = x^3 + Ax + B$)

Définition. On dit que E/K a bonne réduction en v si la courbe

$$\tilde{E}_v : y^2 + \overline{a_1} xy + \overline{a_3} y = x^3 + \overline{a_2} x^2 + \overline{a_4} x + \overline{a_6}$$

(avec $\mathcal{O}_v \to k_v = \mathcal{O}_v / \mathfrak{m}_v$)

est lisse (c'est-à-dire ne contient pas de point singulier).

Sinon, on dit que E a mauvaise réduction en v. Il y a bonne réduction pour presque tout $v \in M_K^0$.

Théorème : Soit $v \in M_K^0$ et soit m premier à la caractéristique de k_v. Supposons que E ait bonne réduction en v. Alors l'application de réduction $E(K) \longrightarrow \tilde{E}_v(k_v)$ induit un isomorphisme

$$E(K)[m] \xrightarrow{\sim} \tilde{E}_v(k_v)[m].$$

À l'aide de ce théorème, on peut analyser l'extension $L = K(\overline{[m]}^{-1}E(K))$ dont on souhaite montrer la finitude.

Proposition :

(a) $\mathrm{Gal}(L/K)$ est abélien et tout élément est d'ordre $|m$

(b) Soit

$$S = \{v \in M_K^0 \mid E \text{ a mauvaise réduction en } v\} \cup \{v \in M_K^0 \mid v(m) \neq 0\}$$

$$\cup\, M_K^\infty$$

Alors L/K est non ramifiée en tout $v \notin S$.

Démonstration : (a) suit de l'injection

$$\begin{aligned} \mathrm{Gal}(L/K) &\longrightarrow \mathrm{Hom}(E(K), E[m]) \\ \sigma &\longmapsto K(\cdot, \sigma) \end{aligned}$$

puisque le groupe à droite est abélien et l'ordre de tout élément divise m.

(b) Soit $v \in M_K \setminus S$. Soit $Q \in E(\bar{K})$ avec $[m]Q \in E(K)$. Il suffit de démontrer que l'extension $K' = K(Q)/K$ est non ramifiée en v. Considérons

$$\begin{array}{ccc} v' \in M_{K'} & & K'_{v'}/K_v \text{ extension de corps résiduels} \\ | & & \\ v \in M_K & & \sim : E(K') \longrightarrow \tilde{E}(K'_{v'}) \end{array}$$

$I_{v'/v} = \ker\left(\mathrm{Gal}(K'_{v'}/K_v) \to \mathrm{Gal}(k'_{v'}/k_v)\right)$ réduction (bonne en v')
(complété à la réduction)

$I_{v'/v} \subset \mathrm{Gal}(\bar{K}/K)$ le groupe d'inertie. Si $\sigma \in I_{v'/v}$, alors

$$\widetilde{\sigma(Q) - Q} = \sigma(\tilde{Q}) - \tilde{Q} = \tilde{O}$$

puisque par définition σ agit trivialement sur $k'_{v'}$.

Par ailleurs,

$$[m]\left(\sigma(Q)-Q\right) = \sigma([m]Q) - \sigma(Q) = 0$$

et donc $\sigma(Q)-Q \in E[m]$ appartient au noyau de la réduction modulo v'. Par le théorème, $\sigma(Q)-Q = 0$. C'est-à-dire, Q est fixé par tous les éléments du groupe d'inertie $\Rightarrow K'/K$ est non ramifiée en v □

⟶ On peut alors appliquer un résultat de finitude de la théorie algébrique des nombres, à savoir :

Théorème : Soit K un corps de nombres. Soit $S \subset M_K$ un ensemble fini contenant M_K^∞ et $m \geq 2$ un entier. L'extension maximale L/K telle que :

* $\mathrm{Gal}(L/K)$ est abélien
* tout élément de $\mathrm{Gal}(L/K)$ est d'ordre $|m$
* L/K est non ramifiée en dehors de S

est finie.

Preuve de Mordell-Weil faible

Soit $L = K\left([m]^{-1}E(K)\right)$. L'extension de l'anneau parfait

$$E(K)/mE(K) \times \mathrm{Gal}(L/K) \longrightarrow E[m]$$

montre que $E(K)/mE(K)$ est fini $\Leftrightarrow$ $\mathrm{Gal}(L/K)$ est fini. Or d'après le théorème précédent, c'est le cas $\square$

$\longrightarrow$ On obtient maintenant déduire de la finitude de $E(K)/mE(K)$ que $E(K)$ est de type fini. C'est à travers du théorème suivant :

Théorème : Soit A un groupe abélien tel que A/mA soit fini. Supposons qu'il existe une fonction

$$h : A \longrightarrow \mathbb{R}$$

avec les propriétés suivantes :

1) Soit $Q \in A$. Il existe $C_1 = C_1(A, Q)$ tel que

$$h(P+Q) \leq 2h(P) + C_1 \quad \text{pour tout } P \in A$$

2) Il existe $C_2 = C_2(A)$ tel que

$$h(mP) \geq m^2 h(P) - C_2 \quad \text{pour tout } P \in A$$

3) Pour tout C_3, l'ensemble

$$\{P \in A \mid h(1) \in C_3\} \text{ est fini.}$$

Alors A est de type fini.

Démonstration : Soient $Q_1, \dots, Q_r \in A$ des représentants de A/mA. Soit $P \in A$.

On écrit :

$$P = mP_1 + Q_{i_1}$$
$$P_1 = mP_2 + Q_{i_2}$$
$$\vdots$$
$$P_{n-1} = mP_n + Q_{i_n}$$

pour des indices $1 \leq i_j \leq r$. On a alors :

$$h(P_j) \underset{(2)}{\leq} \frac{1}{m^2}\left(h(mP_j) + C_2\right)$$
$$= \frac{1}{m^2}\left(h(P_{j-1} - Q_{i_j}) + C_2\right)$$
$$\underset{(1)}{\leq} \frac{1}{m^2}\left(2h(P_{j-1}) + C_1' + C_2\right)$$

avec C_1' le max des constantes pour les points $-Q_1, \dots, -Q_2$. Les constantes C_1' et C_2 ne dépendent pas de P.

$$\Rightarrow h(P_n) \leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \dots + \frac{2^{n-1}}{m^2}\right)(C_1' + C_2)$$

$$< \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_1' + C_2}{m^2 - 2}$$

$$\leq \frac{1}{2^n} h(P) + \frac{1}{2}(C_1' + C_2) \qquad (m \geq 2)$$

Pour n assez grand,

$$h(P_n) \leq 1 + \frac{1}{2}(C_1' + C_2)$$

et en utilisant l'identité

$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j}$$

on voit que tout $P \in A$ s'écrit comme combinaison linéaire d'éléments dans l'ensemble fini

$$\{Q_1, \dots, Q_n\} \cup \{Q \in A \mid h(Q) \leq 1 + \frac{C_1' + C_2}{2}\}$$

propriété (3) □

Pour démontrer le théorème de Mordell sur $K = \mathbb{Q}$, il faut donc construire une fonction

$h : E(\mathbb{Q}) \longrightarrow \mathbb{R}$

avec les propriétés 1), 2), 3).

La hauteur de $t = \frac{p}{q} \in \mathbb{Q}$ avec p et q premiers entre eux est

$$H(t) = \max(|p|, |q|)$$

Soit E une cubique elliptique sur $\mathbb{Q}$ d'équation de Weierstrass

$$E : y^2 = x^3 + Ax + B \qquad A, B \in \mathbb{Z}$$

(toujours possible après changement de variables).

Définition : La hauteur logarithmique de $E(\mathbb{Q})$ est définie par

$$h_x : E(\mathbb{Q}) \longrightarrow \mathbb{R}$$

$$P \longmapsto \begin{cases} \log H(x(P)) & P \neq 0 \\ 0 & P = 0 \end{cases}$$

Théorème : La fonction h_x satisfait à :

1) Soit $P_0 \in E(\mathbb{Q})$. Il existe $C_1 = C_1(P, A, B)$

$$h_x(P + P_0) \leq 2h_x(P) + C_1 \quad \forall P \in E(\mathbb{Q})$$

2) Il existe $C_2 = C_2(A,B)$ tel que

$$h_x([2]P) \geq 4h_x(P) - C_2 \quad \forall P \in E(\mathbb{Q})$$

3) Pour tout C_3, l'ensemble

$$\{P \in E(\mathbb{Q}) \mid h_x(P) \leq C_3\}$$

est fini.

Démonstration : 3) Pour tout C, il y a un nbre fini de $t \in \mathbb{Q}$ avec $H(t) \leq C$ (au plus $(2C+1)^2$). Pour chaque valeur de x, il y a au plus deux valeurs de y telles que $(x,y) \in E(\mathbb{Q})$, donc

$$\{P \in E(\mathbb{Q}) \mid h_x(P) \leq C_3\} \text{ est fini.}$$

1) Pour $(x,y) = \left(\frac{r}{s}, \frac{u}{t}\right) \in E(\mathbb{Q})$, avec des fractions irréductibles,

$$y^2 = x^3 + Ax + B \implies \frac{u^2}{t^2} = \frac{r^3}{s^3} + A\frac{r}{s} + B$$

$$u^2 s^3 = t^2(r^3 + Ars^2 + Bs^3)$$

$t^2 \mid u^2 s^3 \implies t^2 \mid s^3$

$s^3 \mid t^2(r^3 + Ars^2 + Bs^3) \implies s^3 \mid t^2$.

si $p \mid s$ $\quad p \mid r^3 + Ars^2 + Bs^3$

$\implies p \mid r$

$$\implies \boxed{s^3 = t^2}$$

d'où $t = e^3$ et $s = e^2$ (pour $e = ts^{-1}$).

Donc $P = (x,y) = \left(\frac{r}{e^2}, \frac{s}{e^3}\right)$ et $P_0 = \left(\frac{r_0}{e_0^2}, \frac{s_0}{e_0^3}\right)$.

On prend $C_1 > \max\left(h_x(P_0), h_x([2]P_0)\right)$ pour que l'inégalité soit vraie pour $P_0 = O$ ou si $P \in \{O, \pm P_0\}$. Rappelons la formule

$$X(P+P_0) = \left(\frac{y-y_0}{x-x_0}\right)^2 - x - x_0$$

$$= \frac{(xx_0+A)(x+x_0)+2B-2yy_0}{(x-x_0)^2}$$

$$= \frac{(zz_0+Ae^2e_0^2)(ze_0^2+z_0e^2)+\cdots}{(ze_0^2-z_0e^2)^2}$$

$$2Be^4e_0^4 - 2ue.s_0e_0$$

et en utilisant les inégalités

$$z \leq H(x(P))$$
$$e \leq H(x(P))^{1/2}$$
$$u \leq c\,H(x(P))^{3/2}$$

on trouve

$$H(x(P+P_0)) \leq C_1' \cdot H(x(P))^2$$

On laisse la preuve de 2) en exercice. □