(Accouplement de Weil mais c'est moche)

5 juillet 2023

Petit rappel : Sur la courbe elliptique E, $D \in Div^0(E)$ est principal ssi

- $\deg(D) = 0$
- Si $D = \sum n_i(P_i)$, $\sum [n_i]P_i = O$ dans E.

(Voir Isogenies.)

Pareil, pour $E_1,\ E_2$ des courbes ell :

$$\begin{aligned} \phi &: E_1 \to E_2 \\ \phi^* &: \mathrm{Pic}(E_2) \to \mathrm{Pic}(E_1) \\ &\quad (Q) \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P) \end{aligned}$$

Aussi, on a $e_\phi(P) = ord_P\ t_{\phi(P)} \circ \phi$ et $ord_P\ f \circ \phi = e_\phi(P) ord_{\phi(P)}\ f$ (faut simplement l'écrire). D'où

$$\mathrm{div}(\phi^*(\mathrm{div}(f))) = \mathrm{div}(f \circ \phi) \tag{$*$}$$

Construction : On prend $T \in E[m]$, $p \nmid m$, et T' t.q $[m]T' = T$. Alors

- $\exists\ f \in \overline{K}(E)$ tel que $\mathrm{div}(f) = m(T) - m(O)$
- $\exists\ g \in \overline{K}(E)$ tel que $\mathrm{div}(g) = [m]^*((T) - (O))$. On le voit avec

$$\mathrm{div}(g) = [m]^*((T) - (O)) = \sum_{R \in E[m]} (T' + R) - \sum_{R \in E[m]} (R)$$

Le degré est clairement 0 et la somme $\sum_{R\in E[m]} T' + R - R = [\#E[m]]\,T' = O$. Maintenant on remarque que

$$\mathbf{div}(f \circ [m]) = \mathbf{div}(g^m) \tag{$**$}$$

par $(*)$. On suppose donc que $f \circ [m] = g^m$. Et on choisit un autre $S \in E[m]$, T est valable aussi.

Maintenant la magie : On a

$$g(X+S)^m = f([m]X + [m]S) = f \circ [m](X) = g(X)^m$$

Puis $(X \mapsto (g(X+S)/g(X))^m) \equiv 1$ d'où pour tout X, $(g(X+S)/g(X)) \in \mu_m(\overline{K})$ donc prend un nombre fini de valeurs et donc est pas surjective donc constante.

Récap :

- à $T \in E[m]$ on trouve un g vérifiant $(**)$.
- à $S \in E[m]$ on obtient $\alpha \equiv (X \mapsto g(X+S)/g(X))$. On remarque que g est unique à constante près et que le quotient est donc indépendant de g.

Ce qui donne un pairing :

$$e_m \ : \ E[m] \times E[m] \to \mu_m \tag{$\circ$}$$

Props :

- e_m **est bilinéaire.** (Pour la linéarité en T on considère h t.q $div(h) = (T + T') - (T) - (T') + (O)$).
- e_m **est alternée**, $e_m(T,T) = 1$ d'où en part $e_m(S,T) = e_m(T,S)^{-1}$. $(\prod_{i=0}^{m-1} g_T \circ \tau_{[i]T'}$ est constante.$(g_[i+1]T = \prod ...))$
- e_m **est non dégénérée**, i.e.

  $$\forall S \ e_m(S,T) = 1 \implies T = O$$

  (g_T se factoriserai en $\lambda_T \circ [m]$, comparer son diviseur)
- e_m **est galois invariante**, i.e. $e_m(S^\sigma, T^\sigma) = e_m(S,T)^\sigma$. ($g_{T^\sigma} = g_T^\sigma$, c'est clair.)

- e_m **est compatible**, i.e. $\forall S \in E[mm'],\ T \in E[m]\ :\ e_{mm'}(S,T) = e_m([m']S,T)$. (Comparer $g_{T,m} \circ [m']$ avec $g_{T,mm'}^{m'}$.)

Ca c'était les props de base maintenant pour $\phi\ :\ E_1 \to E_2$ et $\hat{\phi}$ sa duale :

- ϕ et $\hat{\phi}$ sont **adjointes** pour e_m, i.e. $e_m(\phi(S),T) = e_m(S,\hat{\phi(T)})$. $(\exists\, h\ :\ \mathrm{div}(h) + (\hat{\phi}(P)) - (O) = \phi^*(T) - \phi^*(O)$ et on lie les $e_m)$

- e_m est **surjective** pour chaque m. (via la non dégénérescence.)

Maintenant on obtient facilement, via la **compatibilité**, un pairing sur le module de Tate :

$$e\ :\ T_l(E) \times T_l(E) \to T_l(\mu) \tag{$\circ\circ$}$$

Maintenant si $\phi \in \mathrm{End}(E)$ et $\phi_l = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans la $\mathbb{Z}_l$-base v_1, v_2 de $T_l(E)$. On calcule

$$\begin{aligned}
(e_m(v_1,v_2)^{deg(\phi)} &= e_m([deg(\phi)]v_1, v_2)) \\
&= e_m(\phi v_1, \phi v_2) \\
&= e_m([a]v_1 + [b]v_2, [c]v_1 + [d]v_2) \\
&= e_m(v_1, v_2)^{ad-bc}
\end{aligned}$$

d'où par la non-dégénérescence

- $deg(\phi) = det(\phi_l)$. ($det(\phi_l)$ est indépendant de l)

- $tr(\phi) = tr(\phi_l) = 1 + deg(\phi) + deg(1-\phi)$.