Feuille 7 : Courbes elliptiques, Action de Galois

Soit K un corps parfait. Soit V un $\overline{K}$-espace vectoriel. On dit que $\mathrm{Gal}(\overline{K}/K)$ (noté également G_K) *agit continument* sur V si pour tout $v \in V$ le stablisateur $\{\sigma \in G_K \mid v^\sigma = v\}$ est fermé d'indice fini dans G_K. (Ceci équivaut à dire que l'action $G_K \times V \to V$ est continue pour la topologie discrète sur V).

Exercice 1 (Action de Galois)

1. Montrer que G_K agit continument sur $\overline{K}$ pour son action naturelle.
2. Soit V un $\overline{K}$-espace vectoriel tel que G_K agit continument et de manière compatible à son action sur $\overline{K}$. Posons
$$V_K := V^{G_K} = \{v \in V \mid \forall \sigma \in G_K,\ v^\sigma = v\}.$$
Fixons $v \in V$.
   (a) Montrer qu'il existe une extension galoisienne L/K finie telle que v est fixé par G_L.
   (b) Montrer que v peut s'écrire comme une combinaison linéaire à coefficients dans $\overline{K}$ d'éléments de V_K (on pourra considérer la matrice $(\sigma_i\alpha_j)$ où $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Gal}(L/K)$ et où les α_j forment une base de L/K).
   (c) En déduire que $V \simeq V_K \otimes_K \overline{K}$.
3. Que dire dans le cas de $\mathbb{C}_p$ et de $G_{\mathbb{Q}_p}$?

Exercice 2
1. Montrer que $\mathbb{Q}_p$ n'a pas de sous-groupe discret non nul.
2. Donner une famille infinie d'exemples de sous-groupes discrets de $\mathbb{Q}_p^*$.

Exercice 3
1. Soit $L/K/\mathbb{Q}_p$ une tour d'extensions finies telle que L/K est galoisienne. Soit $(\alpha_i)_i$ une suite de L telle que $\sum_i \alpha_i$, converge. Soit $\sigma \in \mathrm{Gal}(L/K)$. Montrer que
$$\sum_i \alpha_i^\sigma = \left(\sum_i \alpha_i\right)^\sigma.$$
2. Que dire si on remplace $L/K/\mathbb{Q}_p$ par $\mathbb{C}/\mathbb{R}/\mathbb{R}$?
3. Même question avec $\overline{\mathbb{Q}}/\mathbb{Q}/\mathbb{Q}$.

Exercice 4 (Multiplication complexe $\Rightarrow$ action de Galois abélienne) Soit $E/\mathbb{C}$ une courbe elliptique à multiplication complexe par $\mathcal{O}_K$, l'anneau des entiers d'un corps quadratique imaginaire K. On admet que E admet une modèle sur $H = K(j(E))$ et que tous les endomorphismes de E sont définis sur H. On note, pour tout entier $n \geq 1$,
$$\rho_n : G_H \to \mathrm{Aut}(E[n])$$
l'action de Galois sur les points de torsion. On fixe un entier $n \geq 1$ et on note $H_n := H(E[n])$ l'extension de H engendrée par les (coordonnées des) points de $E[n]$.

1. Relier $\mathrm{Ker}\rho_n$ et $\mathrm{Gal}(H_n/H)$.
2. On admet[1] que $E[n]$ est un $\mathcal{O}_K/m\mathcal{O}_K$-module libre de rang 1. Montrer que ρ_n est un morphisme de G_H dans $\mathrm{Aut}_{\mathcal{O}_K/n\mathcal{O}_K}(E[n])$.

[1] cf. Silverman Advanced Topics in the Arithmetic of Elliptic Curves p.103

3. En déduire que $\mathrm{Gal}(H_n/H)$ est abélien.
4. Conclure que $H(E_{\mathrm{tors}})/H$ est abélienne.

Exercice 5 (Critère de potentielle bonne réduction) Soit K un corps local (complet pour une valuation discrète v, parfait de corps résiduel k parfait). Notons I_v le groupe d'inertie de G_K, p la caractéristique de k. Soit E/K une courbe elliptique. On dit que E/K *a potentiellement bonne réduction* si il existe une extension finie de K sur laquelle E à bonne réduction.

1. Soit K' une extension galoisienne finie de K. Montrer que $I_{v'} \subset I_v$ et que le quotient est fini.
2. Montrer que E/K a potentiellement bonne réduction si et seulement si l'action de I_v sur $\mathrm{Aut}(T_\ell(E)$ se factorise à travers un quotient fini pour un (tous les) premier(s) $\ell \neq p$.

Exercice 6 Corps résiduel (du complété) de la clôture algébrique d'un corps ultramétrique)

1. Soit K un corps ultramétrique algébriquement clos. Montrer que sont corps résiduel k_K est algébriquement clos.
2. Montrer que si K est un corps ultramétrique, de clôture algébrique $\overline{K}$, alors $k_{\overline{K}} = \overline{k_K}$.
3. Montrer que si K est ultramétrique et algébriquement clos, de complété $\widehat{K}$, alors $k_K = k_{\widehat{K}}$.

Exercice 7 (CM⇒ potentielle bonne réduction) Soit L un corps de nombres et E/L une courbe elliptique à multiplication complexe par l'anneau des entiers $\mathcal{O}_K$ d'un corps quadratique imaginaire K (comme précédemment on admet que tous les endomorphismes de E sont définis sur le compositum $L \cdot K$). On veut justifier le titre de l'exercice...
Soit v une place de L (correspondant à un idéal maximal $\mathfrak{p}_v$ du complété $\mathcal{O}_{L_v}$). On note L_v le complété de L pour v ; L_v^{ab} son extension abélienne maximale ; I_v le sous-groupe d'inertie de $\mathrm{Gal}(\overline{L}_v/L_v)$ et I_v^{ab} le sous-groupe d'inertie de $\mathrm{Gal}(L_v^{\mathrm{ab}}/L_v)$. On admet [2] que $I_v \simeq \mathcal{O}_v^\times$. Soit enfin, ℓ un premier différent de la caractéristique p, du corps résiduel $k_v = \mathcal{O}_v/\mathfrak{p}_v$.

1. Montrer I_v agit sur $\mathrm{Aut}(T_\ell(E))$ à travers le quotient I_v^{ab}.
2. On note $\mathcal{O}_{v,1}^\times$ le noyau de l'application naturelle : $\mathcal{O}_v^\times \to k_v^\times$. Montrer que le groupe formel $\widehat{\mathbb{G}_m}(\mathfrak{p}_v)$ est isomorphe à $\mathcal{O}_{v,1}^\times$ par l'application
$$\widehat{\mathbb{G}_m}(\mathfrak{p}_v) \to \mathcal{O}_{v,1}^\times \quad x \mapsto 1 + x.$$
3. Montrer que si $\mathcal{F}$ est une loi de groupe formelle sur $\mathfrak{p}_v$ alors l'application identité induit, pour tout entier $n \geq 1$, des isomorphismes
$$\mathcal{F}(\mathfrak{p}_v^n)/\mathcal{F}(\mathfrak{p}_v^{n+1}) \simeq \mathfrak{p}_v^n/\mathfrak{p}_v^{n+1}.$$

[2] c'est non-trivial : il s'agit d'un résultat de la théorie du corps de classes locale

4. En déduire que $\mathcal{O}_{v,1}^{\times}$ est un pro-p-groupe (*i.e.* une limite projective de groupes finis de cardinal une puissance de p).
5. On note $\mathrm{GL}_2(\mathbb{Z}_\ell)_1$ le noyau de l'application naturelle $\mathrm{Aut}(T_\ell(E)) \to \mathrm{Aut}(E[\ell])$. Montrer que
$$\mathrm{GL}_2(\mathbb{Z}_\ell)_1 \simeq \{A \in \mathrm{GL}_2(\mathbb{Z}_\ell) \mid A = \mathrm{Id} \bmod \ell\}.$$
6. Montrer que $\mathrm{GL}_2(\mathbb{Z}_\ell)_1$ est un pro-ℓ-groupe.
7. Montrer qu'il n'existe pas de morphisme non-trivial d'un pro-p-groupe dans un pro-ℓ-groupe.
8. Construire un diagramme exact reliant les divers objets introduits.
9. Déduire de ce diagramme que l'image de $\mathcal{O}_{v,1}^{\times}$ dans $\mathrm{Aut}(T_\ell(E))$ s'injecte dans $GL_2(\mathbb{Z}/\ell\mathbb{Z})$.
10. Déduire de ceci que l'image de I_v dans $\mathrm{Aut}(T_\ell(E))$ est finie.
11. En utilisant un exercice précédent, conclure : E/L a potentiellement bonne réduction en toute place[3].

[3]La preuve présentée ici est appelée *preuve ℓ-adique*. Il existe également une preuve passant par les nombres complexes ainsi qu'une *preuve p-adique* ne faisant pas intervenir de premier auxiliaire ℓ.