Feuille 5 : Frobenius et début de courbes elliptiques

Exercice 1 (Rappels sur le groupe de décomposition et sur Frobenius) Dans la suite on considère une extension E/F galoisienne de corps de nombres, de degré n, de groupe de Galois G. Soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_F$. Le groupe G agit sur les idéaux maximaux $\mathfrak{P}$ de $\mathcal{O}_E$ au-dessus de $\mathfrak{p}$.

1. Montrer que cette action est transitive (on raisonnera par l'absurde en appliquant le lemme Chinois aux idéaux $\mathfrak{P}' \notin \omega(\mathfrak{P})$ et $\sigma(\mathfrak{P})$ pour tout $\sigma \in G$).
2. Fixons désormais un idéal $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. On rappelle que le *groupe de décomposition* de $\mathfrak{P}/\mathfrak{p}$, noté $D(\mathfrak{P}/\mathfrak{p})$, est le stabilisateur de $\mathfrak{P}$ dans G. Rappeler pourquoi (en notant e l'indice de ramification et f le degré résiduel)
$$|D(\mathfrak{P}/\mathfrak{p})| = ef \quad \text{et} \quad \forall \sigma \in G, \quad D(\sigma\mathfrak{P}/\mathfrak{p}) = \sigma D(\mathfrak{P}/\mathfrak{p})\sigma^{-1}.$$
On note $I(\mathfrak{P}/\mathfrak{p})$ le noyau du morphisme naturel φ de $D(\mathfrak{P}/\mathfrak{p})$ vers $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$: c'est le *groupe d'inertie*.
3. Vérifier que $I(\sigma\mathfrak{P}/\mathfrak{p}) = \sigma I(\mathfrak{P}/\mathfrak{p})\sigma^{-1}$.
4. On rappelle (cours) que φ est un morphisme surjectif. En déduire que,
$$|I(\mathfrak{P}/\mathfrak{p})| = e,$$
et donc que si $\mathfrak{p}$ est non-ramifié dans E/F, alors φ est un isomorphisme.
5. On suppose désormais que $\mathfrak{p}$ est non-ramifié dans E/F. On note $\mathrm{Frob}_{\mathfrak{P}}(E/F)$ ou $(\mathfrak{P}, E/F)$ l'unique élément de $D(\mathfrak{P}/\mathfrak{p})$ dont l'image par φ est l'automorphisme de Frobenius pour $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$: on appelle cet automorphisme l'*automorphisme de Frobenius de* $\mathfrak{P}/\mathfrak{p}$. Autrement dit, c'est l'unique $\sigma \in G$ vérifiant :
$$\sigma \in D(\mathfrak{P}/\mathfrak{p}) \quad \text{et} \quad \forall x \in \mathcal{O}_E, \ \sigma(x) = x^{|\mathbb{F}_{\mathfrak{p}}|} \mod \mathfrak{P}.$$
Quel est l'ordre de $\mathrm{Frob}_{\mathfrak{P}}(E/F)$? Vérifier que
$$\forall \sigma \in G, \quad (\sigma\mathfrak{P}, E/F) = \sigma(\mathfrak{P}, E/F)\sigma^{-1}.$$
[Notons que si E/F est abélien, ceci montre que $(\mathfrak{P}, E/F)$ est indépendant du choix de $\mathfrak{P}$ au-dessus de $\mathfrak{p}$: on le note dans ce cas $(\mathfrak{p}, E/F)$ (ou $\mathrm{Frob}_{\mathfrak{p}}(E/F)$ ou même $\mathrm{Frob}_{\mathfrak{p}}$ si le contexte est clair).]
6. Caractériser le fait que $\mathfrak{p}$ est totalement décomposé en terme des Frobenius $\mathrm{Frob}_{\mathfrak{P}}$.
7. Si K est une extension intermédiaire : $F \subset K \subset E$, et si $\mathfrak{p}_K := \mathfrak{P} \cap \mathcal{O}_K$, montrer que
$$\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}_K} = \left(\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}\right)^{f(\mathfrak{p}_K/\mathfrak{p})}.$$

Exercice 2 (Loi de réciprocité quadratique via Frobenius) Soit $\Delta \in \mathbb{Z} - \{0,1\}$ sans facteur carré. On note $K = \mathbb{Q}(\sqrt{\Delta})$ l'extension quadratique d'anneau d'entiers $\mathcal{O}_K$. On rappelle que
$$O_K = \begin{cases} \mathbb{Z}\left[\sqrt{\Delta}\right] & \text{si } \Delta = 2,3 \mod 4 \text{ et dans ce cas } d_K = 4\Delta. \\ \mathbb{Z}\left[\frac{1+\sqrt{\Delta}}{2}\right] & \text{si } \Delta = 1 \mod 4 \text{ et dans ce cas } d_K = \Delta. \end{cases}$$
Dans la suite on fixe un nombre premier p impair, ne divisant pas Δ (i.e. non-ramifié). Soit par ailleurs ζ une racine primitive p-ième de l'unité et $F = \mathbb{Q}(\zeta)$.

1. En étudiant l'anneau $\mathcal{O}_K/p\mathcal{O}_K$, montrer que p est totalement décomposé dans $\mathcal{O}_K$ si et seulement si $\left(\frac{\Delta}{p}\right) = 1$.
2. En déduire la valeur du Frobenius $\mathrm{Frob}_p(K/\mathbb{Q}) \in \mathrm{Gal}(K/\mathbb{Q})$.
3. Montrer que F contient une unique extension quadratique K de $\mathbb{Q}$. Déterminer Δ tel que $F = \mathbb{Q}(\sqrt{\Delta})$.
4. Soit q un nombre premier impair distinct de p.
5. Calculer $(q, F/\mathbb{Q})$ et en déduire $(q, K/\mathbb{Q})_{|F}$.
6. En déduire[1] la loi de réciprocité quadratique :

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right).$$

Exercice 3 Soit $E/\mathbb{C}$ une courbe elliptique, de réseau associé Λ. On note ω_1, ω_2 des générateurs de Λ. On rappelle que l'anneau des endomorphismes de E est isomorphe à $\mathcal{R} := \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\}$. Par ailleurs si $K/\mathbb{Q}$ est un corps de nombres, on dit que $\mathcal{R}$ est un *ordre de* K si c'est un sous-anneau de K, qui est un $\mathbb{Z}$-module de type fini et tel que $\mathcal{R} \otimes \mathbb{Q} = K$. Montrer que

1. Soit $\mathrm{End}(E) = \mathbb{Z}$;
2. Soit $K := \mathbb{Q}(\omega_1/\omega_2)$ est une extension quadratique imaginaire de $\mathbb{Q}$ et $\mathrm{End}(E)$ est isomorphe à un ordre de K.

Exercice 4 Soit K un corps de caractéristique 0 et ℓ un nombre premier. Pour tout entier $n \geq 1$ on note $\mu_{\ell^n} \subset \overline{K}^*$ le groupe des racines ℓ^n-ieme de 1. L'application $x \mapsto x^\ell$ permet de définir la limite projective (justifier) des μ_{ℓ^n} : on note $T_\ell(\mu)$ cette limite projective (c'est le module de Tate de μ).

1. Décrire $T_\ell(\mu)$ en tant que groupe abstrait.
2. Montrer que l'on a une représentation ℓ-adique naturelle (le *caractère cyclotomique*) de $\mathrm{Gal}(\overline{K}/K)$ vers $\mathrm{Aut}(T_\ell(\mu)) \simeq \mathbb{Z}_\ell^\times$.

Exercice 5 Soit K un corps de caractéristique nulle et ℓ un nombre premier. Montrer que la donnée des accouplements

$$\forall n \geq 1, \quad e_{\ell^n} : E[\ell^n] \times E[\ell^n] \to \mu_{\ell^n}$$

donne naissance à un accouplement de Weil ℓ-adique au niveau des modules de Tate.

Exercice 6 Soient E/K une courbe elliptique sur un corps K de caractéristique 0, et $n \geq 1$.

1. En utilisant le formalisme de l'accouplement de Weil, montrer qu'il existe des points $P, Q \in E[n]$ tels que $e_n(P, Q)$ est une racine primitive n-ieme de l'unité.
2. En déduire que si K est tel que $E[n] \subset E(K)$ alors $\mu_n \subset K^\times$.

Exercice 7 Montrer que le groupe $E(\mathbb{R})$ des points $\mathbb{R}$-rationnels d'une courbe elliptique n'est pas de type fini (alors que l'on sait par un théorème de Mordell que $E(K)$ est de type fini si K est un corps de nombres).

[1] On rappelle que -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p = 1 \mod 4$.