Examen

1. Le théorème de Kronecker-Weber

On désigne par ζ_n une racine primitive n-ième de 1.
Il existe deux versions du théorème de Kronecker-Weber :

Théorème 1. *Soit $K/\mathbb{Q}$ une extension abélienne finie. Alors il existe un entier n tel que $K \subset \mathbb{Q}(\zeta_n)$.*

Théorème 2. *Soit p un nombre premier, et soit $K/\mathbb{Q}_p$ une extension abélienne finie. Alors il existe un entier n tel que $K \subset \mathbb{Q}_p(\zeta_n)$.*

Le but de cet exercice est de montrer que le théorème 1 découle du théorème 2. On admettra donc le théorème 2 dans tout l'exercice (notons que la preuve du théorème 2 est accessible avec les outils vus en cours mais elle est trop longue pour tenir sur cette feuille d'examen).

On fixe dans la suite une extension abélienne finie $K/\mathbb{Q}$.

1. Soit p un nombre premier, et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ au-dessus de p. On note $K_\mathfrak{p}$ le complété de K en $\mathfrak{p}$. Montrer que $K_\mathfrak{p}$ ne dépend pas, à isomorphisme près, du choix de $\mathfrak{p}|p$. On notera dans la suite K_p pour ce complété.

2. Montrer que $K_p/\mathbb{Q}_p$ est une extension abélienne finie.

Il existe donc un entier n_p tel que $K_p \subset \mathbb{Q}_p(\zeta_{n_p})$. On écrit $n_p = m_p p^{e_p}$ avec m_p premier à p.

3. Montrer que si $K/\mathbb{Q}$ est non ramifiée en p on peut prendre $e_p = 0$, ce qu'on supposera par la suite.

4. On pose $n = \prod_p p^{e_p}$. Montrer que l'expression est bien définie.

5. On pose $L = K(\zeta_n)$. Montrer que L est une extension abélienne finie de $\mathbb{Q}$.

6. Montrer qu'un premier p est ramifié dans $L/\mathbb{Q}$ si et seulement si il l'est dans $K/\mathbb{Q}$ (on pourra commencer par montrer que L_p est isomorphe à $K_p(\zeta_n)$).

7. On note I_p le sous-groupe d'inertie de $\mathrm{Gal}(L/\mathbb{Q})$ en p. Montrer que cette définition a un sens.

8. Soit I le sous-groupe de $\mathrm{Gal}(L/\mathbb{Q})$ engendré par les I_p. Montrer que le cardinal de I est $\leq [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$.

9. On note F le sous-corps de L fixé par I. Montrer que $F/\mathbb{Q}$ n'est ramifiée en aucun premier p, et en déduire que $I = \mathrm{Gal}(L/\mathbb{Q})$.

10. Montrer que $L = \mathbb{Q}(\zeta_n)$ et conclure.

2. Extensions modérément ramifiées

Soit p un nombre premier, K une extension finie de $\mathbb{Q}_p$, et L une extension finie de K. On dit que L/K est modérément ramifiée si $e_{L/K}$ est premier à p. Les questions **2.** et **3.** sont indépendantes.

1. Soit L/K une extension finie totalement ramifiée et modérément ramifiée, et $e = [L:K]$. Le but de cette question est de montrer qu'il existe une uniformisante π de K et une racine α de $X^e - \pi$ telles que $L = K(\alpha)$.

a. Soit π_0 une uniformisante de K et β une uniformisante de L. Montrer qu'il existe $u \in \mathcal{O}_L^*$ tel que $\beta^e = u\pi_0$.

b. Montrer qu'il existe $u_0 \in \mathcal{O}_K^*$ tel que $u - u_0 \in \mathfrak{m}_L$.

c. Montrer qu'il existe $v \in L$ avec $v^e = u/u_0$, et conclure.

2. Soit K une extension finie de $\mathbb{Q}_p$. Montrer que $K/\mathbb{Q}_p$ est modérément ramifiée si et seulement si il existe deux entiers n et m premiers à p, et un choix de $p^{1/m}$ une racine m-ième de p, tels que $K \subset \mathbb{Q}_p(\zeta_n, p^{1/m})$.

3. Montrer que si L et M sont deux extensions modérément ramifiées du corps K, alors l'extension composée LM est aussi une extension modérément ramifiée de K.

3. Densité polaire

Soit K un corps de nombres. On désigne par $\mathcal{P}_K$ l'ensemble des idéaux premiers de $\mathcal{O}_K$. Soit A une partie de $\mathcal{P}_K$. On définit pour $s \in \mathbb{C}$: $\zeta_{K,A}(s) = \sum_{I \in [A]} N_{K/\mathbb{Q}}(I)^{-s} = \prod_{\mathfrak{p} \in A}(1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s})^{-1}$, où $[A]$ est le semi-groupe des idéaux de $\mathcal{O}_K$ engendré par A.

1. Montrer que la série définissant $\zeta_{K,A}(s)$ converge absolument et définit une fonction holomorphe sur le demi-plan $\Re(s) > 1$.

2. S'il existe un entier $n > 0$, et un entier $m \geq 0$, tels que $\zeta_{K,A}^n$ s'étende en une fonction méromorphe sur un voisinage de $s = 1$ et ait un pôle d'ordre m en $s = 1$, on dit que A a pour densité polaire $d(A) = m/n$.

a. Montrer que si A a une densité polaire, la valeur de $d(A)$ ne dépend pas du choix de l'entier n tel que $\zeta_{K,A}^n$ s'étende en une fonction méromorphe sur un voisinage de $s = 1$.

b. Montrer que pour $A = \mathcal{P}_K$, A a une densité polaire et que $d(A) = 1$.

c. Soit A une partie de $\mathcal{P}_K$ telle que pour tout $\mathfrak{p} \in A$, $N_{K/\mathbb{Q}}(\mathfrak{p})$ n'est pas premier. Montrer que A a une densité polaire et que $d(A) = 0$.

d. Soit $A \subset A'$ deux parties de $\mathcal{P}_K$, telles que si $\mathfrak{p} \in A' \setminus A$, alors $N_{K/\mathbb{Q}}(\mathfrak{p})$ n'est pas premier. Montrer que A a une densité polaire si et seulement si A' en a une et qu'alors $d(A) = d(A')$.

Soit L/K une extension finie. On dit que $\mathfrak{p} \in \mathcal{P}_K$ est totalement décomposé dans L si pour tout premier $\mathfrak{p}'$ de L au-dessus de $\mathfrak{p}$, on a $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$.

3. Soit L/K une extension galoisienne finie. On note A_L l'ensemble des éléments de $\mathcal{P}_K$ qui sont totalement décomposés dans L. Montrer que A_L a une densité polaire et que $d(A_L) = 1/[L:K]$. (on pourra considérer B l'ensemble des premiers de L au-dessus des éléments de A_L et comparer ζ_{K,A_L} à $\zeta_{L,B}$).

4. Soit L/K et M/K deux extensions galoisiennes finies.

a. Montrer que $\mathfrak{p} \in \mathcal{P}_K$ est totalement décomposé dans l'extension composée LM si et seulement si il est totalement décomposé dans L et dans M.

b. On note A_L (respectivement A_M) l'ensemble des éléments de $\mathcal{P}_K$ qui sont totalement décomposés dans L (respectivement dans M). Montrer que $A_L = A_M$ si et seulement si $L = M$.