TD 5 : Extensions galoisiennes de corps de nombres

Exercice 1. [Groupes de décomposition et d'inertie, résultats de base]

Soit L/K une extension galoisienne de corps de nombres et $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. On fixe $\mathfrak{q}$ un idéal premier de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$, et on note e, f et r les indices de ramification, inertie et décomposition de $\mathfrak{p}$ dans L.

(a) Rappeler la définition du groupe de décomposition $D_\mathfrak{q}$ et du groupe d'inertie $I_\mathfrak{q}$, et donner leurs cardinaux.

(b) Décrire ces groupes pour tout nombre premier, dans le cas des extensions quadratiques de $\mathbb{Q}$.

On considère maintenant la tour d'extensions $K \subset L^{D_\mathfrak{q}} \subset L^{I_\mathfrak{q}} \subset L$, en notant $\mathfrak{q}_D = \mathfrak{q} \cap L^{D_\mathfrak{q}}$ et $\mathfrak{q}_I = \mathfrak{q} \cap L^{I_\mathfrak{q}}$.

(c) Montrer que $[L^{D_\mathfrak{q}} : K] = r$, et que $\mathfrak{p}$ est totalement décomposé dans $L^{D_\mathfrak{q}}$.

(d) Montrer que $[L^{I_\mathfrak{q}} : L^{D_\mathfrak{q}}] = f$ et que $\mathfrak{q}_D$ est inerte dans $L^{I_\mathfrak{q}}$.

(e) Montrer que $[L : L^{I_\mathfrak{q}}] = e$ et que $\mathfrak{q}_I$ est totalement ramifié dans L.

(f) Pour K' une extension intermédiaire entre K et L et $\mathfrak{q}' = \mathfrak{q} \cap K'$, montrer que $\mathfrak{q}'$ est non ramifié sur $\mathfrak{p}$ si et seulement si $K' \subset L^{I_\mathfrak{q}}$, et qu'il est non ramifié et sans inertie sur $\mathfrak{p}$ si et seulement si $K' \subset L^{D_\mathfrak{q}}$.

Exercice 2. [Applications de la théorie]

Dans cet exercice, on utilise les résultats précédents.

(a) Montrer que pour tout extension de corps de nombres L/K (pas nécessairement galoisienne) et tout idéal premier non nul $\mathfrak{p}$ de K, il existe des extensions intermédiaires $K \subset K_D \subset K_I \subset L$ telles que $\mathfrak{p}$ est totalement décomposé dans K' si et seulement si $K' \subset K_D$ et que $\mathfrak{p}$ est non ramifié dans K' si et seulement si $K' \subset K_I$. Montrer de plus que K_D/K et K_I/K sont galoisiennes si L/K l'est.

(b) Grâce à la question précédente, si L et M sont des extensions de corps de nombres de K, montrer que si $\mathfrak{p}$ est non ramifié dans L et M, alors il est non ramifié dans LM, et la même chose pour la décomposition totale.

(c) Trouver des contre-exemples pour la ramification totale et l'inertie.

Exercice 3. [Le cas cyclotomique]

Soit $n \geq 1$, $K = \mathbb{Q}(\zeta_n)$ et p un nombre premier.

(a) On note $\chi : \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ l'isomorphisme habituel. Montrer que pour p ne divisant pas n, le groupe de décomposition D_p est exactement $\chi^{-1}(\langle p \rangle)$.

(b) (*Optionnel, plus difficile*) Décrire D_p et I_p si p divise n.

(c) Déduire du (a) quels nombres premiers sont totalement décomposés (resp. inertes) dans $\mathbb{Q}(\zeta_n)$.

Exercice 4. [Utilisation du Frobenius pour calculer des groupes de Galois]

(a) Soit P un polynôme séparable unitaire à coefficients dans un corps fini k et $n_1, \cdots, n_r$ les degrés des polynômes irréductibles facteurs de P dans $k[X]$. Montrer que le morphisme de Frobenius du corps de décomposition ℓ de P induit une permutation des racines de P dans ℓ de type $(n_1, \cdots, n_r)$, c'est-à-dire dont les longueurs des cycles sont exactement $n_1, \cdots, n_r$.

(b) Soit P un polynôme irréductible unitaire dans $\mathbb{Z}[X]$, K son corps de décomposition sur $\mathbb{Q}$ et p un nombre premier tel que $\overline{P} = P \mod p$ est séparable. On indexe les racines de P par $x_1, \cdots, x_n$. Montrer que le Frobenius en p (défini à conjugaison près) dans $G = \mathrm{Gal}(K/\mathbb{Q})$ induit une permutation de même type que le morphisme de Frobenius sur le corps résiduel.

(c) Soit $P = X^5 - X - 1 \in \mathbb{Z}[X]$. Montrer que P est irréductible, et que le groupe de Galois de son corps de décomposition est $\mathfrak{S}_5$.