TD 9 : 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 $\mathcal{O}_K$.

(a) Rappeler la définition du groupe de décomposition $D_\mathfrak{q}$ et du groupe d'inertie $I_\mathfrak{q}$ pour $\mathfrak{q}$ un idéal de L au-dessus de $\mathfrak{p}$, et donner leurs cardinaux.

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

(c) Donner l'inertie intermédiaire et la ramification intermédiaire de $\mathfrak{p}$ à $\mathfrak{q}$ dans la tour d'extensions $K \subset L^{D_\mathfrak{q}} \subset L^{I_\mathfrak{q}} \subset L$.

(d) 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 l'exercice précédent.

(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. [D'autres résultats élémentaires d'extensions galoisiennes]

Soit L/K une extension galoisienne de corps de nombres de groupe de Galois G, et $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$.

(a) Montrer que si $\mathfrak{p}$ est totalement ramifié dans toute sous-extension stricte L'/K de L/K, alors il l'est dans L/K à moins que G soit cyclique d'ordre premier.

(b) Montrer que si $\mathfrak{p}$ est en-dessous d'un unique idéal premier dans toute sous-extension stricte L'/L de L/K, alors c'est encore le cas dans L/K à moins que G soit cyclique d'ordre premier.

(c) Supposons que $\mathfrak{p}$ n'est ramifié dans aucune sous-extension stricte L'/K de L/K mais ramifié dans L. Montrer que G admet un unique sous-groupe non trivial minimal pour l'inclusion, que celui-ci est cyclique d'ordre premier p pour un certain p, puis que G est un p-groupe.

Exercice 4. [Le cas cyclotomique]

Soit $n \geq 1$, $K = \mathbb{Q}(\zeta_n)$ et p un nombre premier. Cet exercice reprend des éléments du cours sur la réciprocité.

(a) On note $\chi : \mathrm{Gal}(K/\mathbb{Q}) \sim (\mathbb{Z}/n\mathbb{Z})^*$ 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 $\mathbb{Q}(\zeta_n)$.