TD 12 : Extensions galoisiennes de corps de nombres. Révisions

Exercice 1. [Quelques résultats d'extensions galoisiennes]

Soient K,L et M des corps de nombres avec L et M contenant K, et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$.

(a) Montrer que si $\mathfrak{p}$ est non ramifié dans L et dans M, il est non ramifié dans LM.

(b) Montrer que si $\mathfrak{p}$ est totalement décomposé dans L et dans L, il est totalement décomposé dans LM.

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

Exercice 2. [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 inerte dans L, G est cyclique.

(b) Soit $\mathfrak{P}$ un idéal de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$. Montrer que l'extension $L/L^{I_{\mathfrak{P}}}$ est totalement ramifiée en $\mathfrak{P}$ et que $L/L^{D_{\mathfrak{P}}}$ admet un unique idéal premier au-dessus de $\mathfrak{P} \cap \mathcal{O}_{L^{D_{\mathfrak{P}}}}$.

(c) 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.

(d) 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.

(e) 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 3. [Nombres constructibles]

Un nombre complexe est dit constructible si on peut faire des constructions à la règle et au compas pour obtenir celui-ci en partant simplement de 0 et 1. Nous allons ici seulement utiliser que $\alpha \in \mathbb{C}$ est constructible si et seulement si il existe une tour d'extensions quadratiques $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_d = \mathbb{Q}(\alpha)$.

Le but de cet exercice est de comprendre quelles racines de l'unité sont constructibles (théorème de Gauss-Wantzel).

(a) Soit $n \in \mathbb{N}^*$, écrire le degré de $\zeta_n = e^{2i\pi/n}$ en fonction de la décomposition en facteurs premiers de n. En déduire une condition nécessaire à la constructibilité, et donner le premier exemple de racine de l'unité non constructible.

(b) Réciproquement, si n est de la forme nécessaire, montrer que $\mathbb{Q}(\zeta_n)$ est bien obtenue par une tour d'extensions quadratiques. En déduire le théorème.