

DM 2

À remettre le 15 avril.

Exercice.

1. Soit K une extension galoisienne de $\mathbb{Q}$ d'anneau des entiers $\mathcal{O}_K$. On suppose qu'il existe un nombre premier p inerte dans K , i.e. tel que $p\mathcal{O}_K$ soit un idéal maximal de $\mathcal{O}_K$. Montrer qu'alors le groupe de Galois de $K/\mathbb{Q}$ est cyclique (*considérer les groupes de décomposition et d'inertie de l'idéal $p\mathcal{O}_K$*).
2. Soient $K \subset K' \subset K''$ trois corps de nombres emboîtés, $\mathfrak{p}''$ un idéal maximal de K'' , $\mathfrak{p}' = \mathfrak{p}'' \cap K'$ et $\mathfrak{p} = \mathfrak{p}' \cap K$. On note e (resp. e' , e'') l'indice de ramification de $\mathfrak{p}''$ sur K (resp. de $\mathfrak{p}'$ sur K , resp de $\mathfrak{p}''$ sur K') ; on note f (resp. f' , f'') le degré résiduel de $\mathfrak{p}''$ sur K (resp. de $\mathfrak{p}'$ sur K , resp de $\mathfrak{p}''$ sur K'). Montrer que $e = e'e''$ et $f = f'f''$.

Problème. On vérifie sans difficulté que le polynôme $P(X) = X^3 - X + 1$ n'a pas de racine rationnelle, et qu'il est donc irréductible dans $\mathbb{Q}[X]$. Par ailleurs, l'étude des variations de la fonction $x \mapsto P(x)$ montre que ce polynôme admet une unique racine réelle, que l'on note x dans la suite. Le corps $K = \mathbb{Q}[x]$ est donc une extension cubique de $\mathbb{Q}$. Soient y et $\bar{y}$ les deux autres racines de $P(X)$ dans $\mathbb{C}$.

1. Montrer que $y + \bar{y} = -x$, $y\bar{y} = -\frac{1}{x}$ et

$$[(y - x)(\bar{y} - x)(y - \bar{y})]^2 = -23.$$

En déduire que $K[\sqrt{-23}] = \mathbb{Q}[x, y, \bar{y}]$, et que ce corps est une extension galoisienne de degré 6, que l'on notera L dans la suite. Déterminer son groupe de Galois G (*noter qu'un $\mathbb{Q}$ -automorphisme de L est déterminé par son action sur x , y et $\bar{y}$*).

2. Déterminer tous les sous-groupes de G et les sous-extensions de $L/\mathbb{Q}$ correspondantes. Parmi celles-ci, lesquelles sont galoisiennes ?
3. Quels sont les nombres premiers inertes dans l'extension $L/\mathbb{Q}$? (*utiliser la question 1 de l'exercice.*)
4. Montrer que l'anneau des entiers $\mathcal{O}_K$ de K est égal à $\mathbb{Z}[x]$.
5. Montrer que 23 est le seul nombre premier ramifié dans K , et déterminer explicitement la décomposition de l'idéal $23\mathcal{O}_K$ en produits d'idéaux maximaux de $\mathcal{O}_K$. Montrer également que 23 est le seul nombre premier ramifié dans $\mathbb{Q}[\sqrt{-23}]$.
6. Dédurre de la question précédente que 23 est le seul nombre premier ramifié dans L , et que l'indice de ramification correspondant est 2 (*utiliser la question 2 de l'exercice, ainsi que la décomposition de $23\mathcal{O}_K$ obtenue à la question précédente et la relation $efg = [L : \mathbb{Q}]$ vue en cours*).
7. Montrer que l'extension $L/\mathbb{Q}[\sqrt{-23}]$ est non ramifiée, i.e. aucun idéal premier de $\mathbb{Q}[\sqrt{-23}]$ ne se ramifie dans L .