Examen

15/11/17, durée 3h

Les documents sont interdits.

Exercice 1. Les questions suivantes n'ont besoin que de brèves justifications.

1. Rappeler la définition d'une algèbre simple centrale. Soit K/k une extension finie de corps de caractéristique différente de 2. Soit A une k-algèbre. Montrer que A est une algèbre de quaternions si et seulement si $A \otimes_k K$ est une algèbre de quaternions.
2. Soit A et B deux ordres d'une même algèbre à division D de dimension finie sur $\mathbb{Q}$. Soit x un élément de $A \cap B$. Montrer que x est inversible dans A si et seulement si x est inversible dans B.
3. Soit A un anneau d'entier de corps de nombres, et soit n un entier. Montrer qu'il n'existe qu'un nombre fini de classes d'isomorphismes de A-modules M sans torsion tels que $\dim(M \otimes_A \mathrm{Frac}(A)) = n$. Montrer que ce nombre ne dépend pas de n.

Problème

La première partie est indépendante des deux suivantes.

Partie 1.

Soit k un corps. Si P est un polynôme à coefficients dans k, on rappelle que le discriminant de P est le produit des $(\alpha_i - \alpha_j)$, où les α_i sont les racines de P dans une clôture algébrique de k.

1. Soit $P = X^2 + bX + c$ un polynôme unitaire de degré 2 à coefficients dans k. Calculer son discriminant en fonction de b et c.
2. Soit A un anneau intègre, k son corps des fractions, et soit K une extension de K de degré 2. Soit x un élément de K. Montrer que x est entier sur A si et seulement si sa trace et sa norme appartiennent à A.
3. Soit d un entier (positif ou non) que l'on suppose sans facteur carré. Calculer l'anneau des entiers de $\mathbb{Q}[\sqrt{d}]$. On pourra distinguer suivant la valeur de d modulo 4.
4. Soit p un nombre premier impair. Montrer que p est ramifié dans $\mathbb{Q}[\sqrt{d}]$ si et seulement si p divise d.
5. Déterminer pour quelles valeurs de d le nombre premier 2 est ramifié dans $\mathbb{Q}[\sqrt{d}]$.

6. Fixons maintenant deux entiers strictement positifs, impairs, premiers entre eux, sans facteurs carrés d_1 et d_2. Soit $d = -d_1 d_2$. On suppose que d_1 et d_2 sont congrus à 1 modulo 4. Montrer qu'aucun idéal premier de l'anneau des entiers de $k = \mathbb{Q}[\sqrt{-d}]$ n'est ramifié dans $K = \mathbb{Q}[\sqrt{-d_1}, \sqrt{d_2}]$.
7. Montrer qu'il n'existe pas d'élément α de $\mathcal{O}_K$ tel que $\mathcal{O}_K = \mathcal{O}_k[\alpha]$. On pourra calculer le groupe des unités de $\mathcal{O}_k$, puis considérer le discriminant du polynôme minimal de α.

Partie 2. Soit k un corps, et soit K une extension galoisienne de K. On suppose le groupe de Galois G cyclique d'ordre n. Soit σ un générateur de G.

1. On considère K comme un k-espace vectoriel V de dimension n. Soit

$$T : V \to V, x \mapsto \sigma(x).$$

Calculer les valeurs propres de T. On pourra pour cela considérer l'endomorphisme correspondant de $V \otimes_k K$.

2. Soit a un élément de K tel que $N_{K/k}(a) = 1$, et soit

$$R : V \to V, x \mapsto a\sigma(x).$$

Montrer que 1 est valeur propre de R.

3. Montrer le théorème 90 de Hilbert : si a est un élément de K de norme 1, il existe un élément x de K tel que

$$a = \frac{x}{\sigma(x)}.$$

Partie 3. Soit k un corps de nombres de la forme $k = \mathbb{Q}[\sqrt{d}]$ avec $d < 0$. Soit K une extension galoisienne de degré 3 de k, et soit σ l'un des deux générateurs du groupe de Galois de K sur k. On suppose que k ne contient pas de racine cubique de l'unité autre que 1.

1. Soit M un $\mathbb{Z}$-module libre de rang r, et soit $T : M \to M$ un endomorphisme tel que $T^3 = \mathrm{Id}_M$. On suppose que 1 n'est pas valeur propre de T. Montrer que $(\mathrm{Id} - T)(M)$ est un sous-groupe strict de M, dont l'indice est divisible par 3. On pourra considérer les normes des valeurs propres de $\mathrm{Id} - T$.
2. Quel est le rang du groupe des unités de k ?
3. Quel est le rang du groupe des unités de K ?
4. Montrer que l'on peut choisir une unité ω de $\mathcal{O}_K$ dont la norme est 1, telle qu'il n'existe pas d'unité ϵ de $\mathcal{O}_K$ telle que

$$x = \frac{\epsilon}{\sigma(\epsilon)}.$$

5. Montrer qu'il existe un élément y de $\mathcal{O}_K$ tel que $x = \frac{y}{\sigma(y)}$.
6. On suppose qu'aucun idéal premier de $\mathcal{O}_k$ n'est ramifié dans $\mathcal{O}_K$. Montrer que l'idéal (y) est de la forme $I\mathcal{O}_K$, où I est un idéal de $\mathcal{O}_k$. On pourra considérer les diviseurs premiers de (y) et leur comportement sous l'action de σ.
7. Montrer que I n'est pas principal.
8. Montrer que le nombre de classe de k est divisible par 3. On pourra utiliser la notion de norme d'idéaux.
9. Que dire si 3 est remplacé par un nombre premier impair ℓ ?