Université Paris Cité
Sorbonne Université
Master de Mathématiques

Théorie algébrique des nombres I
Année 2024-25
R. Brasca, L. Merel

EXAMEN du 29 octobre 2024

Durée : 3h

Tout appareil électronique et tout document sont interdits, exceptée une feuille manuscrite. Les dépendances entre les parties sont indiquées là où elles peuvent intervenir.

I

Soit K un corps décomposition du polynôme X^3-2 sur $\mathbf{Q}$. Posons $G=\mathrm{Gal}(K/\mathbf{Q})$. Pour p premier non ramifié dans K, notons $C(p)$ la classe de conjugaison dans G d'une substitution de Frobenius en p. Notons d le degré de l'extension $K|\mathbf{Q}$.

1. Montrer que le polynôme X^3-2 est irréductible sur $\mathbf{Q}$.
2. Montrer que K contient une racine cubique primitive de 1, notée j, et que $K=\mathbf{Q}(\alpha,j)$ où $\alpha\in K$ vérifie $\alpha^3-2=0$.
3. En déduire que $d=6$. Quels sont les nombres de plongements réels et complexes non réels de K ?
4. Notons μ_3 le groupe formé par les racines cubiques de l'unité dans $\mathbf{Q}(j)$. Montrer que l'application $\mathrm{Gal}(K/\mathbf{Q}(j))\to\mu_3$ qui à σ associe $\sigma(\alpha)/\alpha$ est un isomorphisme de groupes. En déduire que $\mathrm{Gal}(K/\mathbf{Q})$ est un groupe d'ordre 6. Il est engendré par deux éléments τ et ϵ, qui vérifient $\tau^3=1$, $\epsilon\tau\epsilon=\tau^{-1}$ et $\epsilon^2=1$. On pourra caractériser τ et ϵ par $\tau(\alpha)=j\alpha$, $\tau(j)=j$, $\epsilon(j)=j^{-1}$ et $\epsilon(\alpha)=\alpha$.
5. Montrer que les extensions $\mathbf{Q}(\alpha)|\mathbf{Q}$ et $\mathbf{Q}(j)|\mathbf{Q}$ sont non ramifiées en dehors de 2 et 3. En déduire que l'extension $K|\mathbf{Q}$ est non ramifiée en dehors de 2 et 3.
6. Montrer que les classes de conjugaison de G sont $C_1=\{1\}$, $C_2=\{\tau,\tau^{-1}\}$, $C_3=\{\epsilon,\epsilon\tau,\epsilon\tau^2\}$.
7. Soit p un nombre premier >3.
7.a Montrer que $C(p)=C_1$ si et seulement si on a simultanément que 2 est un cube modulo p et que -3 est un carré modulo p. Ou encore si et seulement si on a $p\equiv 1 \pmod 3$ et $2^{(p-1)/3}\equiv 1 \pmod p$.
7.b Montrer que $C(p)=C_2$ si et seulement si on a simultanément que -3 est un carré et 2 n'est pas un cube modulo p. Ou encore si et seulement si on a $p\equiv 1 \pmod 3$ et on n'a pas $2^{(p-1)/3}\equiv 1 \pmod p$.
7.c Montrer que $C(p)=C_3$ si et seulement si on a simultanément que -3 n'est pas un carré modulo p et que 2 est un cube modulo p. Ou encore si et seulement si on a $p\equiv -1 \pmod 3$.
8. Calculer les densités analytiques des ensembles de nombres premiers $\{p/C(p)=C_i\}$, pour $i=1$, 2, 3. Dans chaque cas, indiquer le degré résiduel en p de l'extension $K|\mathbf{Q}$.

II

Soit K un corps de nombres. Notons $\mathcal{O}_K$ son anneau d'entiers et $d = [K : \mathbf{Q}]$ son degré. Soit r un entier ≥ 1. On dit que $\mathcal{O}_K$ est *engendré par r éléments comme* $\mathbf{Z}$*-algèbre* s'il existe $(\alpha_1, \alpha_2, ..., \alpha_r) \in \mathcal{O}_K^r$ tel que l'application $\mathbf{Z}[X_1, ..., X_r] \to \mathcal{O}_K$ qui à P associe $P(\alpha_1, ..., \alpha_r)$ est surjective.

Soit p un nombre premier totalement décomposé dans K (*i.e.* p est non ramifié dans K et tous les idéaux premiers de $\mathcal{O}_K$ au-dessus de p sont de degré résiduel égal à 1). On note $\mathbf{F}_p$ le corps à p éléments.

Supposons que $\mathcal{O}_K$ est engendré par r éléments comme $\mathbf{Z}$-algèbre.

1. Montrer qu'il existe p totalement décomposé dans K.
2. Montrer qu'il existe un morphisme surjectif d'anneaux $\mathbf{F}_p[X_1, ..., X_r] \to \mathcal{O}_K/p\mathcal{O}_K$.
3. Montrer que l'anneau $\mathcal{O}_K/p\mathcal{O}_K$ est isomorphe à $\mathbf{F}_p^d$.
4. Montrer que l'anneau $\mathbf{F}_p[X_1, ..., X_r]$ possède p^r idéaux maximaux de corps résiduel $\mathbf{F}_p$.
5. En déduire que $d \leq p^r$.

III

On reprend les notations de la partie **II**. On ne suppose plus que $\mathcal{O}_K$ est engendré par r éléments comme $\mathbf{Z}$-algèbre.

Soit l un nombre premier. Soit ζ est une racine primitive l-ème de l'unité. Notons $\mathbf{Q}(\zeta)$ le corps cyclotomique engendré par ζ. On rappelle que son anneau des entiers est $\mathbf{Z}[\zeta]$, que $\mathbf{Q}(\zeta)|\mathbf{Q}$ est une extension abélienne, dont le groupe de Galois s'identifie à $(\mathbf{Z}/l\mathbf{Z})^\times$ par $i + l\mathbf{Z} \mapsto (\zeta \mapsto \zeta^i)$. Notons $\mathbf{Q}(\zeta)^+$ le sous-corps de $\mathbf{Q}(\zeta)$ formé par les invariants sous le groupe $\{-1, 1\} \subset (\mathbf{Z}/l\mathbf{Z})^\times \simeq \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$.

1. Montrer que l'anneau des entiers de $\mathbf{Q}(\zeta)^+$ est engendré par 1 élément comme $\mathbf{Z}$-algèbre.
2. Montrer qu'il existe un corps cubique dont l'anneau des entiers est engendré par 1 élément comme $\mathbf{Z}$-algèbre.
3. Quels sont les nombres premiers p et l tels que $\mathbf{Q}(\zeta)$ contienne un corps cubique K (*i.e.* de degré 3 sur $\mathbf{Q}$) et p totalement décomposé dans K ?
4. Pour $p = 2$, y a-t-il une infinité de tels nombres premiers l ? (On pourra utiliser la partie **I**.)
5. Donner un exemple de corps cubique K tel que $\mathcal{O}_K$ n'est pas engendré par 1 élément comme $\mathbf{Z}$-algèbre. (On pourra utiliser la partie **II**.)
6. Montrer que $\mathbf{Q}(\zeta)$ admet un sous-corps K de degré d sur $\mathbf{Q}$ avec p totalement décomposé dans K si et seulement si $l \equiv 1 \pmod{d}$ et $p^{(l-1)/d} \equiv 1 \pmod{l}$.
7. Montrer que cette dernière condition est satisfaite si et seulement si l est totalement décomposé dans un corps de décomposition du polynôme $X^d - p$.
8. Montrer qu'il existe une extension abélienne K de $\mathbf{Q}$ telle que $\mathcal{O}_K$ n'est pas engendré par r éléments comme $\mathbf{Z}$-algèbre. (On pourra utiliser la partie **II**.)