École Polytechnique

Contrôle classant du 16 avril 2008 MATH 451 Théorie de Galois

Durée 3 heures

Avertissement

Les calculatrices et documents autres que le polycopié de cours et les feuilles, corrigés d'exercices du cours, sont interdits. Il est interdit d'utiliser les téléphones portables durant l'épreuve. La rédaction doit être concise et précise. On énoncera clairement les théorèmes utilisés : toute réponse non justifiée sera considérée comme incorrecte. Il est fortement recommandé de lire le sujet en entier.

Exercice 1.[Degré 3]

Soit $P = X^3 + pX + q, p, q \in \mathbf{Q}$ et $K \subset \mathbf{C}$ l'extension de $\mathbf{Q}$ engendrée par les racines complexes z_1, z_2, z_3 de P. On note $G = \mathrm{Gal}(K/\mathbf{Q})$.

1) Montrer la formule $\mathrm{disc}(P) = (-1)^{\frac{n(n-1)}{2}} \prod_i P'(z_i)$. En déduire la formule $\mathrm{disc}(P) = -4p^3 - 27q^2$.

2) Montrer que P est réductible sur $\mathbf{Q}$ si et seulement si il a une racine dans $\mathbf{Q}$. Si P est réductible, déterminer G en fonction du nombre de racines rationnelles.

On suppose désormais P est racine dans $\mathbf{Q}$ et on plonge G dans S_3 en le faisant agir sur ses racines.

3) Quels sont les sous-groupes de S_3 ?

4) Calculer G en fonction des valeurs de $\mathrm{disc}(P)$.

5) Déterminer tous les sous-corps de K suivant les valeurs de $\mathrm{disc}(P)$.

6) Montrer que P est irréductible sur $\mathbf{Q}(\sqrt{\mathrm{disc}(P)})$.

Exercice 2.[Extensions cycliques]

Soit n un entier ≥ 1 et G le groupe additif $\mathbf{Z}/n\mathbf{Z}$.

1) Démontrer que pour tout diviseur positif d de n, il existe un unique sous-groupe G_d de cardinal d. Montrer que G_d est cyclique et décrire un générateur.

2) Montrer que G_d est distingué dans G et montrer que le quotient est cyclique. Préciser son cardinal.

Soit $K/\mathbf{Q}$ une extension galoisienne de groupe G et $x \in K$ engendrant l'extension. On note P le polynôme minimal de x (sur $\mathbf{Q}$).

3) Justifier l'existence de x. Quelle propriété remarquable possède le polynôme P ?

4) Montrez que, suivant la parité de n, le corps K a un unique sous-corps L tel que $[K : L] = 2$ (resp. $[L : \mathbf{Q}] = 2$) ou bien aucun.

5) Montrer que L/K et $K/\mathbf{Q}$ sont galoisiennes et calculer les groupes de Galois correspondants.

Notons $\sigma \in \mathrm{Aut}(\mathbf{C})$ la conjugaison complexe.

6) Montrer l'égalité $\sigma(K) = K$.

Supposons dans les deux questions suivantes n impair.

7) Montrer que le discriminant de P est le carré d'un nombre rationnel.

8) Montrer que la restriction de σ à K est l'identité.

Supposons $n = 4$ pair $K \not\subset \mathbf{R}$ et soit L' le sous-corps de K fixé par σ.

9) Montrer qu'on a $L = L'$ et $L \subset \mathbf{R}$ (cf. question 4).

10) En déduire que si $m \in \mathbf{Q}$ vérifie $\sqrt{m} \in K$, alors $m \geq 0$.

Exercice 3.[Cyclotomie] Soit n un entier ≥ 1 et $\zeta = \exp(\frac{2i\mathfrak{p}i}{n})$. Soit p premier ne divisant pas n. Pour tout corps k, on note $\mu_n(k)$ le groupe multiplicatif des racines n-ièmes de 1 dans k. On note $(\mathbf{Z}/n\mathbf{Z})^*$ le groupe multiplicatif des inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$.

1) Montrer que $X^n - 1 \in \mathbf{F}_p[X]$ est à racines simples dans $\bar{\mathbf{F}}_p$.

Soit $K = \mathbf{Q}[\zeta], A = \mathbf{Z}[\zeta]$ et $\mathfrak{p}$ un idéal maximal de A contenant p. On note κ le corps fini $\kappa(\mathfrak{p}) = A/\mathfrak{p}$.

2) Montrer que l'application $\xi \mapsto \bar{\xi} = (\xi \mod \mathfrak{p})$ définit un isomorphisme de $\mu_n(K) \to \mu_n(\kappa)$ et que ces groupes sont cycliques d'ordre n. Montrer que $\bar{\zeta}$ est d'ordre n.

3) Rappeler pourquoi $K/\mathbf{Q}$ et $\kappa/\mathbf{F}_p$ sont galoisiennes. Démontrer que les données de $\zeta, \bar{\zeta}$ définissent des plongements $G = \mathrm{Gal}(K/\mathbf{Q}) \subset (\mathbf{Z}/n\mathbf{Z})^*$ et $\bar{G} = \mathrm{Gal}(K/\mathbf{Q}) \subset (\mathbf{Z}/n\mathbf{Z})^*$.

On identifie dorénavant $G, \bar{G}$ à des sous-groupes de $(\mathbf{Z}/n\mathbf{Z})^*$.

4) Montrer que le morphisme composé $D(\mathfrak{p}) \to G \to (\mathbf{Z}/n\mathbf{Z})^*$ s'identifie à la composition des flèches naturelles $D(\mathfrak{p}) \to \bar{G} \to (\mathbf{Z}/n\mathbf{Z})^*$.

5) Montrer qu'il existe un unique $F_\mathfrak{p} \in D(\mathfrak{p})$ d'image le Frobenius dans $\bar{G}$. Montrer que l'image de $F_\mathfrak{p}$ dans $G \subset (\mathbf{Z}/n\mathbf{Z})^*$ est $p \mod n$.

6) En déduire $G = (\mathbf{Z}/n\mathbf{Z})^*$.

7) Déduire de la question précédente que le polynôme cyclotomique $\Phi_n(X) = \prod_{\substack{(m,n)=1 \\ 1 \leq m \leq n}} (X - \exp(\frac{2i\mathfrak{p}i}{n}))$ est irréductible sur $\mathbf{Q}$ (sans utiliser celle du polycopié).

8) Montrer que si $\mathfrak{q}$ est idéal maximal contenant p, on a $F_\mathfrak{p} = F_\mathfrak{q}$.