École Polytechnique

Contrôle classant du 29 avril 2009 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. Il est fortement recommandé de lire le sujet en entier.

Exercice 1.[Un groupe de Galois commutatif]

1) Montrer, par exemple par un calcul brutal, que $5+\sqrt{21}$ n'est pas un carré dans $\mathbf{Q}[\sqrt{21}]$ [Poser $5+\sqrt{21} = (a+b\sqrt{21})^2, a, b \in \mathbf{Q}$ et chercher les valeurs possibles pour a^2].

Soit $z = \sqrt{5+\sqrt{21}}$ et $K = \mathbf{Q}[z]$.

2) Montrer $[K : \mathbf{Q}] = 4$.

3) Soit $z' = \sqrt{5-\sqrt{21}}$. Montrer $z' \in K$ [Calculer zz']. En déduire les conjugués (sur $\mathbf{Q}$) de z puis que $K/\mathbf{Q}$ est galoisienne.

Soit $G = \mathrm{Gal}(K/\mathbf{Q})$.

4) Montrer qu'il existe un unique élément $g \in G$ tel que $g(z) = -z$.

5) Montrer qu'il existe un unique élément $h \in G$ tel que $h(z) = z'$.

6) Montrer qu'on a $g(z') = -z'$ et $h(z') = z$. En déduire que g et h commutent puis $G \simeq (\mathbf{Z}/2\mathbf{Z})^2$.

7) Décrire les sous-corps de K (on précisera un élément primitif pour chacune des extensions de $\mathbf{Q}$ correspondantes).

8) Montrer (sans calcul de préférence) que z ne peut s'écrire sans utiliser de radicaux emboîtés.

9) **Bonus** Peut-on écrire z comme une racine 4-ième d'un rationnel ?

Exercice 2.[Un groupe de Galois non commutatif]

Soit $P(X) = \prod_{i=1}^{n}(X - x_i)$ un polynôme de $\mathbf{Q}[X]$ de degré $n \geq 1$ et notons $y_1, \cdots, y_{n-1} \in \mathbf{C}$ les racines complexes (éventuellement confondues) de $P'(X)$.

1) Montrer la formule

$$\mathrm{disc}(P) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} P'(x_i).$$

En déduire la formule

$$\mathrm{disc}(P) = n^n (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n-1} P(y_i).$$

2) Montrer que le discriminant de $X^n + aX + b$ vaut

$$(-1)^{\frac{n(n-1)}{2}}((1-n)^{n-1}a^n + n^n b^{n-1}).$$

On évitera de passer trop de temps sur les calculs des deux questions précédentes.

Soit $P(X) = X^5 + 20X + 16$ et G son groupe de Galois sur $\mathbf{Q}$.

3) Montrer que les racines complexes de P sont simples.

On choisit une numérotation des racines complexes de P définissant un plongement de G dans S_5.

4) Montrer que P a une unique racine réelle. En déduire que G contient une double transposition.

5) Montrer que G est contenu dans A_5.

6) Factoriser $P(X) \mod 7 \in \mathbf{F}_7[X]$ en facteurs irréductibles [Observer que -2 et -3 sont les seules racines dans $\mathbf{F}_7$]. En déduire que G contient un 3-cycle.

Soit $\bar{P} = P \mod 3 \in \mathbf{F}_3[X]$.

7) Montrer que $\bar{P}$ est sans racine dans $\mathbf{F}_9$ [Observer que pour tout $x \in \mathbf{F}_9^*$ on a $x^5 = \pm x$].

8) En déduire que $\bar{P}$ est irréductible puis que G contient un 5-cycle.

9) Montrer qu'un 3-cycle et une double transposition de S_4 engendrent A_4.

10) Montrer qu'un 5-cycle, un 3-cycle et une double transposition de S_5 engendrent A_5.

11) Montrer que $G = A_5$.

Exercice 3.[Sommes de Gauss et cyclotomie]

1) Soit G un groupe cyclique fini et δ un diviseur de $\mathrm{card}(G)$. Montrer que $G_\delta = \{g^\delta, g \in G\}$ est l'unique sous-groupe de G de cardinal $\mathrm{card}(G)/\delta$.

Soit p un nombre premier > 2 et considérons l'extension cyclotomique de $K/\mathbf{Q}$ (contenue dans $\mathbf{C}/\mathbf{Q}$) avec

$$K = \mathbf{Q}[\zeta],\ \zeta = \exp(\frac{2i\pi}{p}).$$

On note $G = \mathrm{Gal}(K/\mathbf{Q})$.

2) Montrer que $K/\mathbf{Q}$ est galoisienne de groupe de Galois cyclique isomorphe à $(\mathbf{Z}/p\mathbf{Z})^*$.

Soit d un diviseur de $p-1$.

3) Montrer que K contient un unique sous-corps K_d de degré d sur $\mathbf{Q}$.

4) Montrer que K_d sur $\mathbf{Q}$ est galoisienne et qu'on a $K^{G_d} = K_d$.

5) Tout élément de G peut être vu comme un élément de l'espace $\mathrm{End}_{\mathbf{Q}}(K)$ des endomorphismes $\mathbf{Q}$-linéaires de K. Notons $p_d = \frac{d}{p-1}\sum_{g\in G_d} g \in \mathrm{End}_{\mathbf{Q}}(K)$. Montrer la formule

$$gp_d = p_d g = p_d$$

pour tout $g \in G_d$ puis que p_d est un projecteur d'image K_d.

On pose

$$\zeta_d = \sum_{k=0}^{p-1} \zeta^{k^d}.$$

6) Comparer ζ_d et $p_d(\zeta)$. En déduire $\mathbf{Q}[\zeta_d] \subset K_d$.

7) Montrer que $\{g(\zeta), g \in G\}$ est une $\mathbf{Q}$-base de K.

8) Montrer $p_d(g(\zeta)) \in \mathbf{Q}[\zeta_d]$ pour tout $g \in G$ [Observer qu'on a $gp_d = p_d g$ pour tout $g \in G$]. En déduire $K_d = \mathbf{Q}[\zeta_d]$.

9) Montrer $K_{\frac{p-1}{2}} = \mathbf{Q}[\cos(\frac{2\pi}{p})]$.

10) **Bonus** Montrer $K_2 = \mathbf{Q}[\sqrt{\epsilon p}]$ avec $\epsilon = 1$ si -1 carré modulo p et $\epsilon = -1$ sinon.