École Polytechnique

Examen de théorie de Galois du 14 avril 2005

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 précisera clairement les théorèmes utilisés : toute réponse non justifiée sera considérée comme incorrecte. Il est fortement recommandé de lire le sujet en entier. On préférera nettement une copie où certains problèmes sont traités en profondeur plutôt que des questions traitées ça et là sans cohérence. Le problème n'est pas vraiment destiné à être terminé, mais plutôt à donner à chacun la possibilité de montrer ses compétences suivant ses goûts. Ainsi, traiter correctement une bonne moitié du problème donnera une bonne note. On conseille de laisser de côté dans un premier temps les questions « bonus » pour n'y revenir éventuellement qu'après avoir terminé l'ensemble du problème. Elles demandent plus de réflexion indépendante et donc de temps que les autres.

Exercice 1. Soit K le corps $\mathbf{Q}[\sqrt{2}]$.

1) Montrer que si $x \in K$ est un carré (dans K), alors $N_{K/\mathbf{Q}}(x)$ est un carré dans $\mathbf{Q}$. En déduire que $4+2\sqrt{2}$ n'est pas un carré dans K.

Soit L le corps $\mathbf{Q}[\sqrt{4+2\sqrt{2}}]$.

2) Calculer $[L:\mathbf{Q}]$. Quel est le polynôme minimal de $\sqrt{4+2\sqrt{2}}$ sur $\mathbf{Q}$? Sur K ?

3) Montrer que $\sqrt{4-2\sqrt{2}} \in L$. En déduire que $L/\mathbf{Q}$ est galoisienne.

4) Montrer l'existence d'un unique $g \in \mathrm{Gal}(L/\mathbf{Q})$ tel que $g(\sqrt{4+2\sqrt{2}}) = \sqrt{4-2\sqrt{2}}$. Quel est l'ordre de g ?

5) Quels sont les sous-corps de L. Combien y en a-t-il ?

Exercice 2. Soient $d_i, i = 1, \cdots, n$ des nombres rationnels. On suppose que pour tout sous-ensemble non vide J de $\{1, \cdots, n\}$, le produit $\prod_{j\in J} d_j$ n'est pas un carré dans $\mathbf{Q}$. Soit $K_i = \mathbf{Q}[\sqrt{d_1}, \cdots, \sqrt{d_i}]$. On cherche à montrer qu'on a $[K_n : \mathbf{Q}] = 2^n$ par récurrence. On a $K_0 = \mathbf{Q}$.

1) Donner pour tout n un exemple de telle famille $d_i, i = 1, \cdots, n$.

2) Montrer que $K_n/\mathbf{Q}$ est galoisienne.

Supposons $n \geq 1$ et le résultat prouvé pour toute famille de tels d_i de cardinal $\leq n$. Considérons une telle famille de cardinal $n+1$.

3) Montrer que $\mathrm{Gal}(K_n/K_{n-1})$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.

Soit σ non nul dans $\mathrm{Gal}(K_n/K_{n-1})$.

4) Supposons $\sqrt{d_{n+1}} \in K_n$. Montrer qu'on a $\sigma(\sqrt{d_{n+1}}) = \epsilon\sqrt{d_{n+1}}$ avec $\epsilon = \pm 1$.

5) Montrer qu'on a $\sqrt{d_{n+1}} \in K_{n-1}$ si $\epsilon = 1$ et $\sqrt{d_{n+1}d_n} \in K_{n-1}$ si $\epsilon = -1$. En déduire une contradiction et conclure la récurrence.

6) Montrer que l'application

$$\begin{cases} \mathrm{Gal}(K_n/\mathbf{Q}) & \to & \{\pm 1\}^n \\ \sigma & \mapsto & (\sigma(\sqrt{d_1})/\sqrt{d_1}, \cdots, \sigma(\sqrt{d_n})/\sqrt{d_n}) \end{cases}$$

est un isomorphisme de groupes.

7) Montrer que $\mathrm{Gal}(K_n/\mathbf{Q})$ a une (unique) structure de $\mathbf{F}_2$-espace vectoriel compatible à sa structure de groupe. Quelle est sa dimension ?

8) Combien K_n a-t-il de sous-corps de degré 2 sur $\mathbf{Q}$? Pouvez-vous les décrire ?

9) [**Bonus.**] Combien K_n a-t-il de sous-corps ? Pouvez-vous les décrire ?

10) [**Bonus.**] Peut-on plonger d'après vous K_n dans un corps cyclotomique ? Pourquoi ?

Exercice 3.

1) Quel est le groupe de Galois de $\mathbf{Q}[\exp(\frac{2i\pi}{35})]/\mathbf{Q}$? Est-il cyclique ?

2) Combien $\mathbf{Q}[\exp(\frac{2i\pi}{35})]$ a-t-il de sous corps de degré 12 ? De degré 6 ? Pouvez-vous les décrire ?

Exercice 4. Soit k un corps et $z_1, \cdots, z_n \in \bar{k}$ les racines d'un polynôme séparable et unitaire $P \in k[X]$ de degré n et $K = D(P)$ son corps des racines. On rappelle que l'action de $\mathrm{Gal}(K/k)$ sur les racines identifie $\mathrm{Gal}(K/k)$ à un sous-groupe de S_n. Soient p, q désignent deux nombres premiers impairs distincts.

1) Montrer qu'on a

$$\mathrm{disc}(P) = (-1)^{\frac{n(n-1)}{2}} \prod_{k=1}^{n} P'(z_k)$$

où $\mathrm{disc}(P)$ est le discriminant de P. En déduire la formule

$$q^* \stackrel{\text{déf}}{=} \mathrm{disc}(X^q - 1) = (-1)^{\frac{q(q-1)}{2}} q^q.$$

2) On suppose que la caractéristique de k est impaire différente de q ou nulle. Montrer que $X^q - 1$ est séparable. sur k. Montrer que $\mathrm{Gal}(D(X^q - 1)/k)$ est contenu dans A_q si et seulement si q^* est un carré dans k.

On note ζ le complexe $\zeta \stackrel{\text{déf}}{=} \exp(\frac{2i\pi}{q})$ et $G = \mathrm{Gal}(\mathbf{Q}[\zeta]/\mathbf{Q})$ qu'on identifie au groupe cyclique $(\mathbf{Z}/q\mathbf{Z})^*$ comme dans le cours.

3) Montrer que G n'est jamais contenu dans le groupe alterné A_q.

4) Montrer qu'il existe un unique entier $\left(\frac{g}{q}\right)$ de $\{\pm 1\}$ tel que $g^{\frac{q-1}{2}} = \left(\frac{g}{q}\right) \mod q$ pour tout $g \in G = (\mathbf{Z}/q\mathbf{Z})^*$. Par abus, on notera $\left(\frac{p}{q}\right)$ pour $\left(\frac{p \mod q}{q}\right)$.

Soit $H \stackrel{\text{déf}}{=} \{g \in G \text{ tels que } g^{\frac{q-1}{2}} = 1\}$.

5) Montrer que H est l'unique sous-groupe d'indice 2 de G [Montrer d'abord que G est cyclique].

6) Soit γ le morphisme de G dans G définie par $\gamma(g) = g^2$. Quel est le noyau de γ ? Montrer que l'image de γ est contenue dans H. En déduire l'égalité $H = \{g^2, g \in G\}$.

7) Quel est le noyau de la signature $\epsilon : G = (\mathbf{Z}/q\mathbf{Z})^* \to S_q \to \{\pm 1\}$? En déduire la formule $\epsilon(g) = g^{\frac{q-1}{2}}$.

8) Vérifier qu'il existe un unique $\Phi \in G$ tel que $\Phi(\zeta) = \zeta^p$.

9) Montrer que $\Phi \in H$ si et seulement si $p^{\frac{q-1}{2}} = 1 \mod q$. En déduire la formule $\Phi(\sqrt{q^*}) = \left(\frac{p}{q}\right)\sqrt{q^*}$.

Soient A l'anneau $\mathbf{Z}[\zeta]$. On rappelle qu'il existe un idéal premier $\mathfrak{p}$ de A tel que $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. Soit $D_\mathfrak{p} \overset{\text{déf}}{=} \{g \in G \text{ tels que } g^{-1}(\mathfrak{p}) = \mathfrak{p}\}$ le groupe de décomposition de $\mathfrak{p}$.

10) Rappeler pourquoi $\mathbf{F} \overset{\text{déf}}{=} A/\mathfrak{p}$ est un corps fini de caractéristique p. Montrer en utilisant le cours que le morphisme canonique $D_\mathfrak{p} \to \mathrm{Gal}(\mathbf{F}/\mathbf{F}_p)$ est bijectif.

11) [**Plus difficile.**] Montrer que l'image de Φ est le Frobenius de $\mathrm{Gal}(\mathbf{F}/\mathbf{F}_p)$.

12) Montrer que l'action de $\mathrm{Gal}(\mathbf{F}/\mathbf{F}_p)$ sur les $\bar{z}_i = z_i \mod \mathfrak{p}$ induit un plongement de $\mathrm{Gal}(\mathbf{F}/\mathbf{F}_p)$ dans S_q, compatible en un sens qu'on précisera au plongement de $D_\mathfrak{p}$ dans S_q.

13) En déduire que $\Phi \in A_q$ si et seulement si q^* est carré modulo p.

14) Démontrer à l'aide de ce qui précède la loi de réciprocité quadratique

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

15) [**Bonus.**] Pouvez-vous imaginer une démonstration analogue n'introduisant qu'un corps de caractéristique q disons, et pas de corps de caractéristique nulle (en particulier, indépendante de la théorie de la spécialisation du groupe de Galois) ?