École Polytechnique

Contrôle classant du 2 mai 2007 **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.[Racines n-ièmes]

Soit $k(t)$ le corps des fractions rationnelles à coefficients dans un corps k. Soient n, m des entiers > 1. On note ϖ le PPCM de n, m et δ leur PGCD.

1) Montrez que l'équation $x^n = t$ n'a pas de solution $x \in k(t)$ [On pourra écrire $x = P/Q$ avec $\mathrm{PGCD}(P, Q) = 1$].

On note K le corps $\mathbf{C}(t)$ et Ω une clôture algébrique de K. On note enfin K_n l'extension de K engendrée par*une* racine n-ième $\sqrt[n]{t}$ de t dans Ω.

2) Montrer que l'extension K_n/K est galoisienne et calculer son groupe de Galois.

3) Combien K_n a-t-il de sous-corps contenant K ? Pouvez-vous les identifier ?

Soit $H = \mathrm{Gal}(K_{nm}/K)$.

4) Montrer que l'extension K_{nm}/K_n est galoisienne et comparer son groupe de Galois H_n avec H.

Soit K_nK_m le sous-corps de K_{nm} engendré par K_n et K_m.

5) Montrer que l'extension K_{nm}/K_nK_m est galoisienne et calculer son groupe de Galois en fonction de H_n, H_m et H.

6) Comparer K_nK_m et K_ϖ.

7) Montrer que l'extension $K_{nm}/K_n \cap K_m$ est galoisienne et calculer son groupe de Galois en fonction de H_n, H_m et H.

8) Comparer $K_n \cap K_m$ et K_δ.

Exercice 2.[Arithmétique]

Soit n un entier > 0 et ℓ un nombre premier. On dira qu'un entier m n'est pas une ℓ-puissance dans un sous-anneau A de $\mathbf{C}$ si l'équation $x^\ell = m$ n'a pas de solution $x \in A$. On suppose que n n'est pas une ℓ-puissance dans $\mathbf{Z}$.
On note $\zeta = \exp(\frac{2i\pi}{\ell})$ et K le corps de décomposition sur $\mathbf{Q}$ de $P(x) = X^\ell - n$.

1) Montrer l'égalité $K = \mathbf{Q}(\zeta, \sqrt[\ell]{n})$.

2) Soient $x, y \in \mathbf{Q}$ tels que $x^{\ell-1} = y^\ell$. Montrer que x est une ℓ-puissance dans $\mathbf{Q}$. Si de plus x est entier, montrer que x est une ℓ-puissance dans $\mathbf{Z}$.

3) Montrer que n n'est pas une ℓ-puissance dans $\mathbf{Q}[\zeta]$ [Indication : évaluer $N_{\mathbf{Q}[\zeta]/\mathbf{Q}}(n)$ de deux manières].

4) En déduire que P est irréductible sur $\mathbf{Q}[\zeta]$.

Soit G le groupe de Galois de K sur $\mathbf{Q}$.

5) Montrer qu'on a une suite exacte

$$0 \to \mathbf{Z}/\ell\mathbf{Z} \to G \to (\mathbf{Z}/\ell\mathbf{Z})^* \to 1.$$

Soit p un nombre premier différent de ℓ et $F_p \in G$ « un Frobenius » (défini à conjugaison près).

On suppose que P a une racine dans $\mathbf{F}_p$.

6) Montrer que le groupe symétrique $S_{\ell-1}$ n'a pas d'élément d'ordre ℓ. Montrer que le résultat tombe en général en défaut si on ne suppose pas ℓ premier.

7) Montrer que F_p est d'ordre $\neq \ell$.

8) Déduire du théorème de Cebotarev que pour une infinité de nombres premiers p, le polynôme $X^\ell - n$ est sans racine dans $\mathbf{F}_p$.

9) Montrer que si un entier x est une ℓ-puissance dans $\mathbf{F}_p$ pour tout p assez grand, alors x est une ℓ-puissance dans $\mathbf{Z}$.

Exercice 3.[Algèbre] Soit $M \in M_n(k)$ une matrice à coefficients dans k algébriquement clos. On « rappelle » qu'il existe un *unique* couple de matrices $(D,N) \in (M_n(k))^2$ avec D diagonalisable, N nilpotente, $DN = ND$ et $M = D + N$ (décomposition de Jordan-Dunford).

Dans les deux questions suivantes, $k = \mathbf{C}$.

1) Soit $M = \begin{pmatrix} 1 & 2 \\ 0 & z \end{pmatrix}$, $z \in \mathbf{C}$. Calculer D, N comme plus haut suivant les valeurs de z.

2) En déduire que les applications $M \mapsto D$ et $M \mapsto N$ ne sont pas continues.

Soit $M \in M_n(\mathbf{Q})$ et (D,N) sa décomposition de Jordan-Dunford dans $\mathbf{C}$ lorsqu'on voit M comme matrice complexe.

3) Montrer $M, N \in M_n(\bar{\mathbf{Q}})$.

4) Montrer qu'il existe une extension galoisienne finie $K/\mathbf{Q}$ telle que $D, N \in M_n(K)$.

Soit G le groupe de Galois d'une telle extension. On note $g(N), g(D)$ les matrices $[g(n_{i,j})], [g(d_{i,j})]$ où $n_{i,j}, d_{i,j}$ sont les coefficients de D, N.

5) Montrer que D, N sont fixés par G. En déduire $D, N \in M_n(\mathbf{Q})$.

6) Généraliser le résultat précédent au cas des matrices à coefficients dans un corps parfait.

7) Soit $k = \mathbf{F}_2(t)$ et $M = \begin{pmatrix} 0 & t \\ 1 & 0 \end{pmatrix}$. Montrer que les matrices $D, N \in M_2(\bar{k})$ de la décomposition de Dunford de M ne sont pas à coefficients dans k.
