École Polytechnique

Contrôle classant du 30 juin 2006

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.[Un gros groupe de Galois]

Soit $n \geq 2, m$ des entiers naturels.

1) Soit $(a_1, \cdots, a_m)$ un m-cycle de S_n et $\sigma \in S_n$. Montrer la formule

$$\sigma(a_1, \cdots, a_m)\sigma^{-1} = (\sigma(a_1), \cdots, \sigma(a_m)).$$

Soient $s, \sigma \in S_n$ des cycles de longueur respectives $n, n-1$ et $(a, b), 1 \leq a < b \leq n$ une transposition. Soit $\Sigma \subset S_n$ le sous-groupe qu'ils engendrent.

2) Montrer qu'il existe une $i \in \mathbf{N}$ tel que $s^i \sigma s^{-i}$ fixe a.

3) Montrer que $(a, a+1) \in \Sigma$ puis $(i, i+1) \in \Sigma, 1 \leq i < n$.

4) Montrer $\Sigma = S_n$.

5) Soit p un nombre premier. Montrer qu'il existe $P \in \mathbf{F}_p[X]$ irréductible de degré n.

6) Montrer qu'il existe un polynôme **unitaire** $P \in \mathbf{Z}[X]$ et un nombre premier $p > 3$ tel que

– La réduction de P modulo 2 est irréductible ;

– La réduction de P modulo 3 est séparable et a un facteur irréductible de degré $n-1$.

– La réduction modulo p est séparable et a exactement $n-2$ racines dans $\mathbf{F}_p$.

7) Montrer que tout polynôme comme dans la question précédente a groupe de Galois S_n.

Exercice 2.[Un calcul explicite] Soit n un entier ≥ 3. Soit $\zeta \in \mathbf{C}$ une racine primitive n-ième de l'unité.

1) Montrer l'égalité $[\mathbf{Q}[\zeta + \zeta^{-1}] : \mathbf{Q}] = \varphi(n)/2$.

2) Montrer l'égalité $\mathbf{Q}[\zeta + \zeta^{-1}] = \mathbf{R} \cap \mathbf{Q}[\zeta]$.

3) Quelle est l'image de la conjugaison complexe dans $(\mathbf{Z}/n\mathbf{Z})^*$ par le caractère cyclotomique.

4) Montrer que $\mathbf{Q}[\zeta + \zeta^{-1}]/\mathbf{Q}$ est galoisienne et déterminer son groupe de Galois.

5) Soit $x \in \mathbf{Q}$. Calculer $[\mathbf{Q}[\cos(2\pi x)] : \mathbf{Q}]$ en fonction de l'écriture de x sous forme de fraction irréductible d'entiers.

6) Supposons dans cette question $n \neq 4$. Montrer qu'on a

$$[\mathbf{Q}[\sin(\frac{2\pi}{n})] : \mathbf{Q}] = \begin{cases} \varphi(n), & \text{si } \mathrm{pgcd}(n, 8) < 4\,; \\ \varphi(n)/4 & \text{si } \mathrm{pgcd}(n, 8) = 4\,; \\ \varphi(n)/2 & \text{si } \mathrm{pgcd}(n, 8) > 4. \end{cases}$$

7) Montrer que l'aire d'un triangle de $\mathbf{R}^2$ à sommets dans $\mathbf{Q}^2$ est un nombre rationnel.

8) Montrer que les carrés rationnels à sommets dans $\mathbf{Q}^2$ sont les seuls polygones réguliers de $\mathbf{R}^2$ à sommets dans $\mathbf{Q}^2$.

9) Montrer que $i \in \mathbf{Q}[\zeta]$ si et seulement si n est un multiple de 4.

10) On suppose n non multiple de 4. Montrer l'égalité $\mathbf{Q}[\sin(\frac{2\pi}{n}), i] = \mathbf{Q}[\zeta, i]$. En déduire $\mathbf{Q}[\zeta] = \mathbf{Q}[i\sin(\frac{2\pi}{n})]$.

On suppose désormais n multiple de 8.

11) Montrer qu'on a $\sin(\frac{2\pi}{n}) \in \mathbf{Q}[\cos\frac{2\pi}{n})]$. En déduire l'égalité $\mathbf{Q}[\sin(\frac{2\pi}{n})] = \mathbf{Q}[\cos(\frac{2\pi}{n})]$.

12) Calculer les conjugués de $\sin(\frac{2\pi}{n})$ sur $\mathbf{Q}$.

13) **Bonus.** Décrire le sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^*$ correspondant (par la correspondance de Galois) à $\mathbf{Q}[\sin(\frac{2\pi}{n})]$ lorsque $\text{pgcd}(n, 8) = 4, n \neq 4$.

Exercice 3.[Théorème des zéros de Hilbert] Soit $j : A \to B$ un morphisme d'anneaux.. On suppose de plus que B est un A-*module de type fini*. Autrement dit, il existe $b_1, \cdots, b_n$ dans B tel que tout élément de B soit une combinaison linéaire à coefficients dans A des b_i.

1) Montrer que tout élément de B est entier sur A.

Supposons désormais A non nul et B corps et j injectif ce qui permet de considérer A comme un sous-anneau de B.

2) Soit $a \in A - \{0\}$. Montrer qu'il existe $P \in A[X]$ tel que $a^{-1} = P(a) \in B$. En déduire que $P(a) \in A$ est l'inverse de a dans A.

3) Montrer que A est un corps.

On se propose de démontrer le résultat suivant par récurrence sur n. Soit $B = k[x_1, \cdots, x_n]$ une k-algèbre intègre de type fini sur un corps k. Alors, B est un corps si et seulement si $\dim_k(B) < \infty$.

4) Montrer la partie réciproque.

On suppose $n \geq 1$ et le théorème prouvé pour toutes les extensions de corps $K[\xi_1, \cdots, \xi_{n-1}]/K$. On suppose jusqu'à (9) inclus que x_n est transcendant sur k et que $B = k[x_1, \cdots, x_n]$ est un corps.

5) Montrer que la k-algèbre $k[x_n] \hookrightarrow B$ est isomorphe à une algèbre de polynômes sur k et que le plongement $k[x_n] \to B$ se prolonge uniquement en un plongement $k(x_n) = \text{Frac}(k[x_n]) \hookrightarrow B$.

6) Montrer que B est de dimension finie sur $k(x_n)$.

7) Montrer qu'il existe $P \in k[x_n] - \{0\}$ tel que $x_i, i = 1, \cdots, n$ soit entier sur le sous-anneau $k[x_n, P^{-1}] \subset k(x_n)$.

8) Montrer que B est un *module de type fini* sur $k[x_n, P^{-1}]$. En déduire que $k[x_n, P^{-1}]$ est un corps.

9) En considérant $x \in \bar{k}$ n'annulant pas le polynôme P, montrer qu'il existe un unique morphisme surjectif de k-algèbres $k[x_n, P^{-1}] \to k[x]$ qui envoie x_n sur x. Montrer que le noyau est un idéal non nul.

10) En déduire que l'hypothèse x_n transcendant sur k est absurde.

11) Démontrer le théorème annoncé.

12) Montrer que les idéaux maximaux de l'algèbre de polynômes $\mathbf{C}[X_1, \cdots, X_n]$ sont exactement les idéaux $I_x = \{P \in \mathbf{C}[X_1, \cdots, X_n] \text{ tels que } P(x) = 0\}$ où $x = (x_1, \cdots, x_n) \in \mathbf{C}^n$. Montrer que I_x est aussi l'idéal engendré par les monômes $X_i - x_i, i = 1, \cdots, n$.