Université Joseph Fourier
Licence de mathématiques, L3

Mat366 - Algèbre II

Examen du 15 mai 2006

Durée: 4 heures. Pas de document autorisé.
Les questions de **I**, et les parties **II**, **III** sont indépendantes. On peut à tout moment admettre les résultats d'une question pour traiter les suivantes. *Chaque réponse doit être justifiée; la qualité de la rédaction sera un élément important de l'appréciation.*

I Questions indépendantes

1. Soient α_1, α_2, α_3 les trois racines du polynôme complexe $X^3 + aX^2 + bX + c$. Déterminer le nombre $A = {\alpha_1}^2{\alpha_2}^2 + {\alpha_2}^2{\alpha_3}^2 + {\alpha_1}^2{\alpha_3}^2$ en fonction de a, b et c.

2. Soit j le nombre complexe $e^{2\pi i/3}$. On note $\mathbb{Z}[j]$ le sous–anneau de $\mathbb{C}$ image de $\mathbb{Z}[X]$ par le morphisme d'anneaux $P \mapsto P(j)$. Déterminer le corps des fractions de $\mathbb{Z}[j]$.

3. Les corps $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(i\sqrt{2})$ sont–ils isomorphes?

II Corps finis et polynômes

On considère dans $\mathbb{F}_2[X]$ les deux polynômes

$$P_1 = X^5 + X^4 + 1$$
$$\text{et} \quad P_2 = X^5 + X^2 + 1\,.$$

1. Montrer qu'un seul de ces polynômes est irréductible et factoriser l'autre en produit d'irréductibles.

2. Donner une construction du corps $\mathbb{F}_{32}$ comme extension monogène $\mathbb{F}_2(\alpha)$ de $\mathbb{F}_2$. Préciser le polynôme minimal de α sur $\mathbb{F}_2$, puis celui de α^{-1}.

3. Quel est le nombre des polynômes irréductibles de degré 5 sur $\mathbb{F}_2$?

4. Pour $i = 1, 2$ on note K_i un corps de décomposition de P_i sur $\mathbb{F}_2$. Le polynôme $X^2 + X + 1$ est–il irréductible dans $\mathbb{F}_8[X]$? Déterminer chacun des corps finis K_i.

5. Soit H le sous–groupe de ${K_1}^*$ engendré par les racines de P_1.

a) D'après le cours, quelle est la structure du groupe H?

b) Trouver les ordres des racines de P_1 dans ${K_1}^*$ et montrer que deux de ces racines engendrent H. En déduire le cardinal de H.

T.S.V.P.

III Extensions de $\mathbb{Q}$ et leur groupe de Galois

On considère le polynôme $P = X^3 - 3X - 1$ de $\mathbb{Q}[X]$.

1. Montrer que P est irréductible.

2. Montrer que P possède trois racines réelles α_1, α_2, α_3 telles que $\alpha_3 < \alpha_2 < 0 < \alpha_1$.

3. a) Montrer que si α est une racine de P, alors $2 - \alpha^2$ en est une également.

Dans la suite on note $K = \mathbb{Q}(\alpha_1)$.

b) Montrer que l'extension $K \supset \mathbb{Q}$ est galoisienne.

c) Déterminer son groupe de Galois et montrer que tout $g \in \mathrm{Gal}(K|\,\mathbb{Q})$ induit une permutation paire sur $R = \{\alpha_1, \alpha_2, \alpha_3\}$. Justifier que R est une orbite pour l'opération de $\mathrm{Gal}(K|\,\mathbb{Q})$ sur K.

4. Pour chaque i dans $\{1, 2, 3\}$, on désigne par β_i un nombre complexe tel que ${\beta_i}^2 = \alpha_i$, et on suppose les β_i choisis de telle sorte que $\beta_1\beta_2\beta_3 = 1$. On pose $L = K(\beta_1, \beta_2, \beta_3)$.

a) Déterminer $[K(\beta_1) : K]$ (on pourra regarder si α_2, puis α_1 est un carré dans K, en utilisant l'opération du groupe $\mathrm{Gal}(K|\,\mathbb{Q})$).

b) En déduire le polynôme minimal de β_1 sur $\mathbb{Q}$.

c) Montrer que $[L : \mathbb{Q}] = 12$.

5. Montrer que l'extension $L \supset \mathbb{Q}$ est galoisienne. On note $G = \mathrm{Gal}(L|\,\mathbb{Q})$ et $H = \mathrm{Gal}(L|K)$; H est–il un sous–groupe distingué de G?

6. Décrire l'image de β_1 et β_2 par chacun des éléments de H et justifier que H est abélien.

7. Donner la définition de polynôme résoluble par radicaux, et montrer que le polynôme $X^6 - 3X^2 - 1 = P(X^2)$ de $\mathbb{Q}[X]$ est résoluble par radicaux *(cette question ne sert pas en 8.)*.

8. En utilisant 3.c) et 4., montrer que pour tout choix de (ϵ, ϵ') dans$\{1, -1\}^2$, il existe un élément unique de G qui vérifie l'une quelconque des relations (1), (2), (3) suivantes:

$$\begin{array}{lllll} (1) & g(\beta_1) = \epsilon\beta_1 & , & g(\beta_2) = \epsilon'\beta_2 \\ (2) & g(\beta_1) = \epsilon\beta_2 & , & g(\beta_2) = \epsilon'\beta_3 \\ (3) & g(\beta_1) = \epsilon\beta_3 & , & g(\beta_2) = \epsilon'\beta_1 \quad . \end{array}$$

Quel est l'ordre d'un élément g qui vérifie une relation (2) ou (3)? Existe-t-il F sous–corps de L qui soit une extension *galoisienne* de $\mathbb{Q}$ de degré 4? (on pourra utiliser un théorème de Sylow.)