Université Joseph Fourier
Licence LST, L3 mathématiques

Mat365 - Algèbre 3

Examen du 19 mai 2008

Durée: 3 heures. Documents, calculatrices et téléphones portables interdits.
Les quatre exercices sont indépendants. 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 isolées

1) On note x_1, x_2, x_3 les racines du polynôme complexe $P = X^3 + pX + q$. Exprimer le nombre $\sum_{i=1}^{3} x_i^5$ en fonction de p et q.

2) On note F le corps $\mathbb{Q}(i)$. Donner un sous–anneau strict de F dont F est le corps des fractions.

II Une extension de $\mathbb{Q}$

On pose $\alpha = i\sqrt{5+\sqrt{5}}$ et $K = \mathbb{Q}(\alpha)$.

1) Montrer $\mathbb{Q}(\sqrt{5}) \subset K$.

2) Quelle propriété de l'extension $K \supset \mathbb{Q}$ en déduisez-vous?

3) Déterminer le polynôme minimal P de α sur $\mathbb{Q}$ et $[K : \mathbb{Q}]$.

4) Démontrer que l'extension $K \supset \mathbb{Q}$ est galoisienne et donner les différentes images de α par les éléments de $G = \mathrm{Gal}(K \mid \mathbb{Q})$.

5) Déterminer le cardinal et la structure du groupe G.

6) A–t–on $i \in K$? (on pourra utiliser 5) et la correspondance de Galois).

III Corps finis

1) Construire explicitement un corps K à 9 éléments et donner un élément x de K^* qui est d'ordre maximal.

2) Les éléments x et x^{-1} ont–ils alors même polynôme minimal sur $\mathbb{F}_3$?

3) Combien y a–t–il d'éléments d'ordre maximal dans K^*?

4) Déterminer le corps de décomposition D du polynôme $X^3 - 2$ de $\mathbb{F}_p[X]$, pour chacune des valeurs $p = 3$, $p = 5$, $p = 7$.

T.S.V.P.

IV Polynôme irréductible de groupe de Galois $\mathfrak{A}_4$

Pour un polynôme Q de $K[X]$, où K est un corps, on appellera *type de décomposition de Q sur K* la suite croissante des degrés des polynômes irréductibles qui apparaissent dans une factorisation de Q en irréductibles de $K[X]$. Ainsi le type de décomposition de $X^3 - 1$ sur $\mathbb{Q}$ est $(1, 2)$.

Soit P un polynôme *irréductible* de $\mathbb{Q}[X]$, tel que $G = \mathrm{Gal}(P, \mathbb{Q})$ soit isomorphe au groupe alterné $\mathfrak{A}_4$. On note E le sous–corps de $\mathbb{C}$ engendré par les racines de P dans $\mathbb{C}$; ainsi $G = \mathrm{Gal}(E \,|\, \mathbb{Q})$. On rappelle que pour tout sous–groupe H de G, la notation E^H désigne le sous–corps des éléments x de E qui sont fixés par chaque élément de H.

1) Prouver que $\deg P$ divise 12, et $\deg P \geq 4$.

2) Dans cette question on suppose que $\deg P = 12$.

a) Combien le corps $\mathbb{C}$ contient–il de corps de rupture de P distincts?

b) On note H un sous–groupe de G de cardinal 3. Donner le type de décomposition de P sur E^H.

3) On suppose désormais que $\deg P = 4$.

a) Justifier que le groupe $\mathfrak{A}_4$ possède exactement 4 sous-groupes de cardinal 3, qui sont tous conjugués.

b) Si H est un sous–groupe de G et $g \in G$, montrer que $g(E^H) = E^{gHg^{-1}}$.

c) Montrer que E contient exactement 4 corps de rupture de P distincts.

On note K un de ces corps de rupture.

d) Quel est le type de décomposition de P sur K? Que vaut $\mathrm{Gal}(P, K)$?

Soit τ un élément d'ordre 2 de G. On note $F = E^{<\tau>}$.

e) Soit $\alpha \in E$ une racine de P. Montrer que $[F(\alpha) : F] = 2$. Donner le type de décomposition de P sur F.

- ♢ -