Université Joseph Fourier
Licence de mathématiques, L3

Mat366 - Algèbre II

Examen du 30 juin 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. Montrer que l'extension $\mathbb{C}(X) \supset \mathbb{R}(X)$ est finie, et déterminer son degré.

2. Factoriser le polynôme $X^9 - X$ en produit d'irréductibles dans $\mathbb{Q}[X]$, puis dans $\mathbb{F}_3[X]$.

3. a) Construire le corps $\mathbb{F}_4$ et écrire sa table de multiplication.

b) Combien existe-t-il de sous–corps à 4 éléments dans le corps $\mathbb{F}_{64}$?

c) Combien existe-t-il de morphismes de corps de $\mathbb{F}_4$ dans $\mathbb{F}_{64}$?

4. Montrer que le groupe de permutations $\mathfrak{S}_4$ est résoluble.

II Un corps de décomposition et son groupe de Galois

On note γ le nombre complexe $(1+i)\sqrt[4]{5}$.

1. Déterminer le polynôme minimal P de γ sur $\mathbb{Q}$.

2. Déterminer le sous–corps E de $\mathbb{C}$ qui est corps de décomposition de P sur $\mathbb{Q}$. Montrer que $i \in E$ et que $[E : \mathbb{Q}] = 8$.

3. a) Donner la définition d'extension galoisienne, ainsi qu'une deuxième caractérisation équivalente.

b) Soit F un sous–corps de E. L'extension $E \supset F$ est–elle forcément galoisienne? Donner l'exemple d'un sous–corps F tel que $F \supset \mathbb{Q}$ ne soit pas galoisienne.

4. Décrire les éléments du groupe de Galois $G = \mathrm{Gal}(E|\,\mathbb{Q})$ *(cette question n'est pas indispensable pour la suite)*.

5. Le groupe G est–il abélien?

6. Expliciter le groupe $H = \mathrm{Gal}(E|\,\mathbb{Q}(i))$. Le groupe H est–il cyclique?

T.S.V.P.

III Un théorème de Kronecker

On considère un polynôme unitaire $P = \sum_{j=0}^{n} a_j X^j$ de $\mathbb{Z}[X]$, de degré n, tel que $a_0 \neq 0$. On suppose que P est irréductible et que toutes ses racines dans $\mathbb{C}$ sont de module ≤ 1. On souhaite montrer que P est un polynôme cyclotomique.

1. Etablir soigneusement ce résultat sous l'hypothèse qu'une racine de P dans $\mathbb{C}$ est racine N^{e} de l'unité ($N \in \mathbb{N}^*$).

Dans la suite on note $\zeta_1, \ldots, \zeta_n$ les racines de P dans $\mathbb{C}$ et on va prouver que les ζ_i sont des racines de l'unité, ce qui établira le résultat souhaité.

2. En considérant le produit $\zeta_1 \cdots \zeta_n$, montrer que chaque ζ_i est de module 1.

3. Pour $s \in \mathbb{N}$ et $r \in \{1, \ldots, n\}$ on pose dans $\mathbb{Z}[X_1, \ldots, X_n]$

$$T_{r,s} = (-1)^r \sum_{1 \leq k_1 < \cdots < k_r \leq n} (X_{k_1} \cdots X_{k_r})^s \,.$$

a) Le polynôme $T_{r,s}$ est–il symétrique?

b) Reconnaître chaque polynôme $T_{r,1}$. Montrer qu'il existe $U_{r,s} \in \mathbb{Z}[X_1, \ldots, X_n]$ tel que $T_{r,s} = U_{r,s}(T_{1,1}, \ldots, T_{n,1})$.

4. a) Pour $s \in \mathbb{N}$ on pose

$$Q_s(X) = \prod_{i=1}^{n} (X - (\zeta_i)^s)) \,,$$

ainsi $Q_1 = P$. Pour $1 \leq r \leq n$, expliciter le coefficient $b_{r,s}$ de X^{n-r} dans Q_s.

b) Que vaut $T_{r,1}(\zeta_1, \ldots, \zeta_n)$? En déduire $b_{r,s}$ en fonction des coefficients a_j de P.

5. Déduire de 4.a) que $|b_{r,s}| \leq C_n^r$ ($s \in \mathbb{N}$).

6. On note $\mathcal{E}_n$ l'ensemble $\{\sum_{j=0}^{n} c_j X^{n-j} \in \mathbb{Z}[X] \,|\, \forall j, |c_j| \leq C_n^j\}$ et on fixe i dans $\{1, \ldots, n\}$.

a) Justifier que $\mathcal{E}_n$ est un ensemble fini et montrer que l'ensemble $\{(\zeta_i)^s | \, s \in \mathbb{N}\}$ est fini.

b) En déduire qu'il existe $N \in \mathbb{N}^*$ tel que $(\zeta_i)^N = 1$.

- ♢ -