Université Joseph Fourier
Licence LST, L3 mathématiques

Mat366 - Algèbre II

Examen du 21 mai 2007

Durée: 3 heures. Documents et calculatrices interdits.
Les quatre exercices sont indépendants. On peut à tout moment admettre les résultats d'une question pour traiter les suivantes.

I Relations coefficients-racines

On note x_1, x_2, x_3 les racines du polynôme complexe $P = X^3 + aX^2 + bX + c$.

1) Déterminer le polynôme unitaire Q de racines les x_i^2, $i \in \{1, 2, 3\}$ (on *pourra* développer le polynôme $Q(X^2)$).

2) A quelle condition sur a, b et c l'un des x_i^2 est–il la somme des deux autres?

II Etude d'irréductibilité et de résolubilité

On considère le polynôme $P = X^5 - 15X^2 + 1$ de $\mathbb{Q}[X]$.

1) Montrer que la réduction modulo 2, $\overline{P} \in \mathbb{F}_2[X]$, de P n'a pas de racine dans le corps $\mathbb{F}_4$.

2) Le polynôme $\overline{P}$ est–il irréductible dans $\mathbb{F}_2[X]$?

3) Montrer que P est irréductible dans $\mathbb{Q}[X]$.

4) Le polynôme P est–il résoluble par radicaux sur $\mathbb{Q}$? Donner le degré sur $\mathbb{Q}$ d'un corps de décomposition de P.

III Racines de l'unité dans $\overline{\mathbb{F}_p}$

Soit p un nombre premier. On note $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$.

1) Soit x dans $(\overline{\mathbb{F}_p})^*$. Montrer que l'ordre multiplicatif s de x est fini, premier à p.

2) Soit n entier ≥ 1. Montrer que le sous–corps de $\overline{\mathbb{F}_p}$ formé des points fixes sous l'automorphisme $(\mathrm{Fr}_p)^n : x \mapsto x^{p^n}$ de $\overline{\mathbb{F}_p}$ est l'unique sous–corps de cardinal p^n de $\overline{\mathbb{F}_p}$.

Dans la question 3) on pose $q = p^n$ et on note $\mathbb{F}_q$ ce sous–corps.

3) Pour s premier à p, on note μ_s le groupe multiplicatif formé des racines s-ièmes de 1 dans $\overline{\mathbb{F}_p}$. Montrer que $\mathbb{F}_q$ contient le groupe μ_s si et seulement si on a $s \mid q-1$.

4) On revient au 1), on note d l'ordre de la classe de p modulo s, vue comme élément du groupe $(\mathbb{Z}/s\mathbb{Z})^\times$. Montrer l'égalité $\mathbb{F}_p(x) = \mathbb{F}_{p^d}$.

T.S.V.P.

5) *Application numérique* On considère le polynôme $P = X^4 + X^3 + X^2 + X + 1$ dans $\mathbb{F}_{19}[X]$.

a) Soit x une racine de P dans $\overline{\mathbb{F}_{19}}$. Montrer que x est d'ordre 5 dans $(\overline{\mathbb{F}_{19}})^*$.

b) Utiliser 4) pour en déduire les degrés des facteurs irréductibles de P dans $\mathbb{F}_{19}[X]$.

IV Existence d'un élément primitif

Soit $E \supset K$ une extension finie, de caractéristique 0.

1) Justifier qu'il existe $n \geq 1$ et des éléments $\alpha_1, \ldots, \alpha_n$ de E tels que $E = K(\alpha_1, \ldots, \alpha_n)$.

Pour $i \in \{1, \ldots, n\}$, on note P_i le polynôme minimal de α_i sur K et on pose $P = \prod_{i=1}^n P_i$.

2) Montrer l'existence d'un corps L contenant E tel que l'extension $L \supset K$ soit galoisienne.

On note $G = \mathrm{Gal}(L|\, K)$.

3) Utiliser 2) pour montrer que l'ensemble $\mathcal{C}$ des sous–corps de E qui contiennent K est fini. On indiquera l'ensemble fini avec lequel $\mathcal{C}$ est en bijection par la correspondance de Galois.

4) Soient $\alpha, \beta \in E$. On considère les corps $K_t = K(\alpha + t\beta)$, $t \in K$. Déduire de 3) qu'il existe t, t' distincts dans K tels que $K_t = K_{t'}$, et montrer qu'alors $K_t = K(\alpha, \beta)$.

5) Déduire de 1) et 4) que l'extension $E \supset K$ est monogène, c'est–à–dire qu'il existe $\gamma \in E$ tel que $E = K(\gamma)$.

6) Déduire de 5) le nombre de K-morphismes de E dans L.

7) On prend $K = \mathbb{Q}$ et $E = \mathbb{Q}(\sqrt[3]{5}, i)$. Que vaut $[E : \mathbb{Q}]$? Trouver un élément γ de E tel que $E = \mathbb{Q}(\gamma)$.

- $\diamondsuit$ -