HX3 Mathématiques

# Devoir surveillé N$^o$9

Samedi 29 avril 2006

- Durée : 4 heures -

*Les deux problèmes sont totalement indépendants.*

*On laissera une marge à gauche. Seules les conclusions et les résultats mis en valeur seront pris en compte. Enfin, les solutions doivent être rédigées et le formalisme utilisé avec parcimonie.*

## Problème 1 :

On se propose, dans ce problème, de démontrer quelques propriétés des sous-corps du corps des nombres complexes $\mathbb{C}$. On rappelle que, si $K$ est un sous-corps d'un corps $K'$, ce dernier est, en particulier, un $K$-espace vectoriel, ce qui donne un sens à la $K$-dimension de $K'$ notée $\dim_K(K')$.

Si $K$ est un corps, on note $K[X]$ l'anneau des polynômes à coefficients dans $K$. On dit qu'un polynôme de degré strictement positif est *irréductible* s'il ne peut s'écrire comme produit de deux polynômes de degré strictement positif. Un polynôme est *unitaire* si le coefficient de son terme de plus haut degré est égal à 1.

### I. Première partie.

La question **1)** est classique et servira surtout à fixer quelques notations ; la question **2)** n'est pas utilisée dans la suite.

On désigne par $K$ un sous-corps de $\mathbb{C}$, par $\alpha$ un nombre complexe non nul, par $K[\alpha]$ le sous-espace du $K$-espace vectoriel $\mathbb{C}$ engendré par les nombres $\alpha^n$ pour $n \in \mathbb{N}$, enfin par $I_K(\alpha)$ l'ensemble des polynômes de $K[X]$ annulés par $\alpha$.

**1) a.** Montrer que les deux conditions suivantes sont équivalentes :

(i) La $K$-dimension de $K[\alpha]$ est finie.

(ii) $I_K(\alpha) \neq \{0\}$.

Si elles sont remplies, on dit que $\alpha$ est *$K$-algébrique*, ce que l'on suppose dans toute la suite de cette question.

**b.** Montrer qu'il existe un unique polynôme unitaire $P \in K[X]$ tel que tout élément de $I_K(\alpha)$ soit un multiple de $P$, et que $P$ est irréductible.

Ce polynôme $P$ sera noté $\mu_{\alpha,K}$ et appelé *polynôme minimal de $\alpha$ sur $K$*.

**c.** Comparer le degré de $\mu_{\alpha,K}$ et $\dim_K(K[\alpha])$.

**d.** Montrer que $K[\alpha]$ est un corps.

**2)** On prend $K = \mathbb{Q}$.

**a.** Déterminer le polynôme minimal de $\alpha = \sqrt{2}$ sur $\mathbb{Q}$.

**b.** Déterminer le polynôme minimal de $\alpha = \sqrt{\dfrac{1+\sqrt{5}}{2}}$.

## II. Deuxième partie.

On définit $K$ et $\alpha$ comme dans la première partie. On suppose que $\alpha$ est $K$-algébrique et on pose $n = \dim_K(K[\alpha])$.

**1)** Montrer que, si $P$ est un élément irréductible de $K[X]$, ses racines dans $\mathbb{C}$ sont simples.

**2) a.** On note $\lambda_1, \ldots, \lambda_n$ les racines de $\mu_{\alpha,K}$ dans $\mathbb{C}$. Montrer que pour tout $i \in [\![ 1, n ]\!]$, il existe un unique morphisme de $K$-algèbre $\sigma_i$ de $K[\alpha]$ dans $\mathbb{C}$ tel que $\sigma_i(\alpha) = \lambda_i$ (on remarquera qu'un tel morphisme laisse les éléments de $K$ invariants).

**b.** Obtient-on de cette façon tous les morphismes de $K$-algèbres de $K[\alpha]$ dans $\mathbb{C}$ ?

**3)** Montrer que si $\beta$ est un élément de $K[\alpha]$ et si les $\sigma_i(\beta)$ sont deux à deux distincts, alors on a $K[\alpha] = K[\beta]$.

**4)** Etant donné un élément $\beta$ de $K[\alpha]$, démontrer l'existence de deux éléments $\beta_1$ et $\beta_2$ de $K[\alpha]$ vérifiant $K[\beta_1] = K[\beta_2] = K[\alpha]$ et $\beta_1 + \beta_2 = \beta$.
Indication : on pourra introduire, pour $i \neq j$ l'ensemble $E_{i,j}$ des éléments $\lambda$ de $K$ vérifiant :

$$\sigma_i(\alpha + \lambda\beta) = \sigma_j(\alpha + \lambda\beta)$$

## III. Troisième partie.

**1)** Soit $K \subset L \subset M$ trois sous-corps de $\mathbb{C}$. On suppose que $L$ est un $K$-espace vectoriel de dimension finie $n$ et $M$ un $L$-espace vectoriel de dimension $p$. En considérant $(e_1, \ldots, e_n)$ base du $K$-espace vectoriel $L$ et $(f_1, \ldots, f_p)$ base du $L$-espace vectoriel $M$, démontrer que $M$ est un $K$-espace vectoriel de dimension finie $np$.

**2)** On considère deux nombres algébriques sur $\mathbb{Q}$, $\alpha$ et $\beta$. On pose $K = \mathbb{Q}[\alpha]$.

**a.** Comparer $\mathbb{Q}[\alpha\beta]$ et $K[\beta]$.

**b.** Conclure que $\alpha\beta$ est algébrique sur $\mathbb{Q}$.

**c.** Le nombre $\alpha + \beta$ est-il algébrique sur $\mathbb{Q}$ ?

**3)** On pose dans cette question $\alpha = \sqrt{2} + \sqrt[3]{2}$.

**a.** Montrer que $\alpha$ est algébrique.

**b.** Montrer que $\deg \mu_{\alpha,\mathbb{Q}} \leqslant 6$.

**c.** En utilisant la première question, démontrer que $\deg \mu_{\alpha,\mathbb{Q}} = 6$.

On note $\mathbb{A} \subset \mathbb{C}$ l'ensemble des nombres algébriques sur $\mathbb{Q}$.

**4)** Démontrer que $\mathbb{A}$ est un sous-corps de $\mathbb{C}$.

**5)** Démontrer que $\mathbb{A}$ est un corps algébriquemet clos, autrement dit, que si $P \in \mathbb{A}[X]$ est un polynôme non constant, alors $P$ admet une racine dans $\mathbb{A}$.

**6)** Démontrer que $\mathbb{A}$ est dénombrable.

**7)** On appelle *nombre transcendant* un nombre complexe qui n'est pas algébrique. Justifier l'existence de nombres transcendants.

## IV. Quatrième partie.

Soit $S \in \mathbb{Q}[X]$ irréductible sur $\mathbb{Q}$, $\deg S = n \geqslant 2$.

**1)** Démontrer qu'il existe $C_S \in \mathbb{N}^*$ tel que pour tout rationnel $r = p/q$ ($(p, q) \in \mathbb{Z} \times \mathbb{N}^*$) il vienne

$$|S(r)| \geqslant \frac{1}{C_S q^n}$$

**2)** Supposons que $\alpha$ soit une racine réelle de $S$. Déduire du résultat précédent l'existence de $K > 0$ tel que pour tout rationnel $r = p/q$ ($(p, q) \in \mathbb{Z} \times \mathbb{N}^*$) dans $[\alpha - 1, \alpha + 1]$

$$|\alpha - r| \geqslant \frac{K}{q^n}$$

**3)** Pour tout $n \geqslant 0$, on pose

$$t_n = \sum_{k=0}^{n} 10^{-k!}$$

Démontrer que $(t_n)_{n\in\mathbb{N}}$ converge vers un réel $t$. Etablir que si $n \geqslant 0$

$$|t - t_n| \leqslant 2 \times 10^{-(n+1)!}$$

**4)** En déduire que le réel $t$ est transcendant sur $\mathbb{Q}$.

## Problème 2 :

Le but de ce problème est de prouver le théorème de d'Alembert. On suppose donc ce résultat non démontré.

On admettra que $\mathbb{C}$ est contenu dans $M$ un surcorps algébriquement clos. En particulier, tout polynôme non nul de $\mathbb{C}[X]$ est scindé sur $M$.

On admettra également le résultat suivant : soit $K$ est un corps commutatif, $T \in K[X_1, \dots X_n]$. On suppose que $T$ est une expression symétrique de $X_1, \dots, X_n$ ( i.e pour toute permutation $\sigma$ de $[\![ 1, n ]\!]$ , on a $T(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = T(X_1, \dots, X_n)$). Alors, il existe $U \in K[X_1, \dots, X_n]$ tel que

$$T(X_1, \dots, X_n) = U(\Sigma_1, \dots, \Sigma_n)$$

avec $\Sigma_1, \dots, \Sigma_n$ les expressions symétriques élémentaires des $X_i$, autrement dit pour $1 \leqslant k \leqslant n$

$$\Sigma_k = \sum_{1\leqslant i_1<i_2<\ldots<i_k\leqslant n} X_{i_1} X_{i_2} \cdots X_{i_k},$$

et en particulier on a $\Sigma_1 = X_1 + X_2 + \cdots + X_n$, $\Sigma_2 = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n$,... et $\Sigma_n = X_1X_2 \cdots X_n$.

**Préliminaires.**

**1)** Soit $x, y \in M$. On suppose que $x + y \in \mathbb{C}$ et $xy \in \mathbb{C}$. Démontrer que $x$ et $y$ sont dans $\mathbb{C}$.

Soit $P = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{R}[X]$ de degré $n \geqslant 1$. On appelle $\lambda_1, \dots, \lambda_n$ ses racines distinctes ou confondues dans $M$.

**2)** Pour $k \in [\![ 1, n ]\!]$ , exprimer $\Sigma_k(\lambda_1, \dots, \lambda_n)$ en fonction des coefficients de $P$.

**3)** Soit $T \in \mathbb{R}[X_1, \dots X_n]$ une expression symétrique de $X_1, \dots, X_n$. Démontrer que $T(\lambda_1, \dots, \lambda_n) \in \mathbb{R}$.

**4)** On suppose dans cette question que $P = X^n + X - 1$ avec $n \geqslant 4$. Calculer $T(\lambda_1, \dots, \lambda_n)$ lorsque

**a.** $T = X_1 + \cdots + X_n$ ;
**b.** $T = X_1^2 + \cdots + X_n^2$ ;
**c.** $T = X_1^3 + \cdots + X_n^3$.

**I. Première partie.**

Soit $P \in \mathbb{R}[X]$ non constant. Le but de cette partie est de montrer que $P$ admet une racine dans $\mathbb{C}$. On note $n = \deg P$ et on écrit $n = 2^k m$ avec $k \in \mathbb{N}$ et $m$ impair.

**1)** Traiter les cas $k = 0$.

On note $\lambda_1, \dots, \lambda_n$ les racines distinctes ou confondues de $P$ dans $M$. Pour tout réel $c$ et tout couple $(h, k) \in [\![ 1, n ]\!]^2$ avec $h \leqslant k$, on pose

$$y_{hk}(c) = \lambda_h + \lambda_k + c\lambda_h\lambda_k.$$

Enfin, on note $Q_c = \prod_{1 \leqslant h \leqslant k \leqslant n} (X - y_{hk}(c))$.

**2)** On suppose uniquement dans cette question que pour tout réel $c$, $Q_c$ admet une racine complexe.

**a.** Démontrer qu'il existe $(r, s) \in [\![ 1, n ]\!]$ avec $r \leqslant s$ et $c \neq c'$ dans $\mathbb{R}$ tels que $y_{rs}(c)$ et $y_{rs}(c')$ sont dans $\mathbb{C}$.

**b.** Démontrer que $\lambda_r$ et $\lambda_s$ sont dans $\mathbb{C}$.

**3) a.** Justifier que les coefficients de $Q_c$ sont des expressions polynômiales rélles et symétriques des $\lambda_k$.

**b.** En déduire que $Q_c \in \mathbb{R}[X]$.

**4)** Déterminer le degré de $Q_c$. Quel est l'exposant de 2 dans la décomposition de $\deg Q_c$ en produit de nombre premier ?

**5)** Conclure par récurrence que $P$ admet une racine complexe.

## II. Deuxième partie :

Soit $P \in \mathbb{C}[X]$ non constant. En considérant le polynôme $R = P\overline{P}$, démontrer que $P$ admet une racine complexe.