Université de Paris 7 | **Exercices du 30-03-2007** | **agreg 2007 (F.Han)**

Exercice I:

Soit k un corps commutatif.

1) Montrer que si k n'est pas dénombrable, alors $k(X)$ est un k espace vectoriel de dimension infinie non dénombrable.

2) Si k est algébriquement clos et non dénombrable. Soit K une extension de k telle que K soit un k-espace vectoriel de dimension finie ou dénombrable, alors $K = k$.

3) Connaissez vous un corps algébriquement clos dénombrable?

Exercice II: Th des zéros (Nullstellensatz) faible

Soit k un corps algébriquement clos non dénombrable[1]

1) Soit $(a_1, \ldots, a_n)$ un élément de k^n. Montrer que l'idéal $(x_1 - a_1, \ldots, x_n - a_n)$ de $k[x_1, \ldots, x_n]$ est maximal.

2) Soit $\mathcal{M}$ un idéal maximal de $k[x_1, \ldots, x_n]$, déduire de l'exercice précédent qu'il existe $(a_1, \ldots, a_n) \in k^n$ tel que $\mathcal{M} = (x_1 - a_1, \ldots, x_n - a_n)$.

3) Soit I un idéal de $k[x_1, \ldots, x_n]$. On note $V(I) = \{(a_1, \ldots, a_n) | \forall P \in I, P(a_1, \ldots, a_n) = 0\}$.

$$\text{Montrer que } V(I) = \emptyset \iff I = k[x_1, \ldots, x_n]$$

Exercice III: Th des zéros (Nullstellensatz)

Soit k un corps algébriquement clos, que l'on suppose non dénombrable.

1) Soit I un idéal d'un anneau commutatif unitaire A. Montrer que $\sqrt{I} := \{a \in A | \exists n \in \mathbb{N}^*, a^n \in I\}$ est un idéal de A.

2) Nous alons montrer le Théorème: Soit I un idéal de $k[x_1, \ldots, x_n]$, et $V(I)$ le lieu des zéros dans k^n des éléments de I. Alors l'idéal des polynômes qui s'annulent en tous les points de $V(I)$ est $\sqrt{I}$.

a) Soit $I = (P_1, \ldots, P_r)$ un idéal de $k[x_1, ..., x_n]$, et F un élément de $k[x_1, \ldots, x_n]$ nul en tout point de $V(I)$. On considère l'idéal J de $k[x_1, \ldots, x_n, t]$: $J = (1 - t.F, P_1, \ldots, P_r)$. Montrer que $J = k[x_1, \ldots, x_n, t]$.

b) En déduire que $F \in \sqrt{I}$.

3) a) Etudier $V(I + J)$, $V(I \cap J)$, $V(I.J)$.

b) Pour $I \subset J$, comparer $V(I)$ et $V(J)$. Montrer que l'ensemble $(I : J) = \{a \in k[x_1, \ldots, x_n], \forall P \in J, a.P \in I\}$ est un idéal contenant I. Etudier $V(I : J)$.

Exercice IV: [2]

1) Soit A l'anneau des fonctions holomorphes sur $\mathbb{C}$.

a) Soit $n \in \mathbb{N}^*$. Quels sont les zéros complexes de $\sin(\frac{\pi.z}{n})$. En déduire que l'idéal I_n des éléments de A nuls sur $n.\mathbb{Z}$ est principal.

b) Montrer que l'idéal engendré par $\left(\sin(\frac{\pi.z}{n})\right)_{n \in \mathbb{N}^*}$ n'est pas de type fini.

2) On dit qu'un anneau commutatif est noetherien si tout idéal est de type fini. Soit A un anneau Noetherien. Nous allons montrer que $A[x]$ est aussi Noetherien. Soit I un idéal de $A[x]$.

a) On suppose que I n'est pas de type fini. Soit f_1 un élément non nul de I, et pour $n > 0$ on choisit f_{n+1} de plus petit degré parmis les éléments de $I - (f_1, \ldots, f_n)$. On note a_j le coefficient du terme de plus haut degré de f_j. Montrer qu'il existe $m \in \mathbb{N}$ et $(u_i) \in A^m$ tels que $a_{m+1} = \sum_{j=1}^{m} u_j.a_j$.

b) Obtenir une contradiction sur la définition de f_{m+1}.

Exercice V: Codes cycliques

Soit q une puissance d'un nombre premier. Pour $n \in \mathbb{N}, n > 1$, on pose $H = \mathbb{F}_q[X]/(X^n - 1)$.

1) On appellera code cyclique de longueur n un idéal I de H vu comme $\mathbb{F}_q$-espace vectoriel. Montrer que I est principal, et donner une base de I en fonction d'un générateur bien choisi de I.[3]

---

[1] Cf par exemple Francinou-Gianella pour une preuve sans l'hypothèse non dénombrable

[2] CF Mérindol p 259

[3] La matrice des vecteurs de base exprimée dans la base (x^i) est appelée matrice génératrice du code.

2) Codes de Reed-Solomon. On suppose $q > 2$, et l'on pose $n = q - 1$. Soit $t \in \mathbb{N}, 1 < t \leq n$. On note $\Sigma = \{1, \ldots, t-1\}$

a) Montrer qu'il existe dans $\mathbb{F}_q$ une racine primitive n-ième de l'unité (On en choisira une notée ζ).

b) On considère le polynôme $g = \prod_{i \in \Sigma}(X - \zeta^i)$. Montrer que g permet de définir un code cyclique de longueur n. Quelle est sa dimension.

c) Montrer qu'un élément non nul m de l'idéal (g) de $\mathbb{F}_q[X]/(X^n - 1)$ exprimé dans la base $1, \ldots, X^{n-1}$ a au moins t coordonnées non nulles. [4] En déduire que la distance minimale entre 2 mots du code est t.

d) Remarquer que si l'on regarde maintenant ces $\mathbb{F}_q$ espaces vectoriels comme des $\mathbb{F}_p$ espaces vectoriels, alors ce code peut corriger $(t-1)/2 * s$ erreurs consécutives, (où $q = p^s$). Par exemple, deux codes racourcis de celui obtenu par la méthode précédente en prenant $q = 2^8$ et $t = 5$ sont utilisés dans les CD.

[4] Un élément du code (g) est appelé un mot du code. La distance entre 2 mots est le nombre de coordonnées différentes des 2 vecteurs.