Polynômes à une indéterminée

Préparation à l'agrégation interne année 2008-09

Séance du mardi 8 septembre

Exercices à chercher en priorité : 1.1 ; 2.1 ; 2.2 ; 2.3 ; 2.4 ; 2.6 et ceux de la partie 3.

1 Racines et PGCD

Exercice 1.1

1. Soit $\mathbb{K}$ un corps commutatif. Démontrer que si P est un polynôme de $\mathbb{K}[X]$ de degré n ($n \in \mathbb{N}^*$)alors il admet au plus n racines distinctes.
2. (a) On suppose de plus que $\mathbb{K}$ est infini. Démontrer que si P est un polynôme de $\mathbb{K}[X]$ tel que $P(x) = 0$ pour tout $x \in \mathbb{K}$ alors $P = 0$.
   (b) Qu'en est-il si $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier ?

Exercice 1.2 (PGCD de deux polynômes)

1. Déterminer le pgcd de $X^p - 1$ et de $X^q - 1$ dans $\mathbb{R}[X]$ (où p et q désignent des entiers naturels supérieurs ou égaux à 2).
2. On pose $P = X^5 - 13X^4 + 67X^3 - 171X^2 + 216X - 108$; calculer le pgcd de P et P' et en déduire une décomposition de P (indication : calculer le pgcd de P' et de $5P$).

Exercice 1.3

Soit A, B, C trois polynômes appartenant $\mathbb{C}[X]$ deux à deux premiers entre eux tels que :$A^2 + B^2 = C^2$

1. Montrons que $B + C$ et $B - C$ sont des carrés de polynômes.
2. En déduire l'expression des polynômes A, B et C.

Exercice 1.4 (Résultant de deux polynômes)

Soit $\mathbb{K}$ un corps commutatif.

1. *Question préliminaire :* Démontrer que deux polynômes de $\mathbb{K}[X]$ P et Q de degré respectivement m et n au moins égaux à 1.Démontrer que le PGCD de P et Q est de degré supérieur ou égal à 1 si seulement si il existe deux polynômes non nuls $R, S \in \mathbb{K}[X]$ tels que :
$$\begin{cases} deg(R) \leq n-1 \\ deg(S) \leq m-1 \\ PR = QS \end{cases}$$
2. Dans cette question on suppose que $m = 3$ et $n = 2$.
   (a) On pose $P = a_3X^3 + a_2X^2 + a_1X + a_0$ et $Q = b_2X^2 + b_1X + b_0$.Démontrer que P et Q admet un facteur commun de degré ≥ 1 si et seulement si :
$$\begin{vmatrix} a_3 & 0 & b_2 & 0 & 0 \\ a_2 & a_3 & b_1 & b_2 & 0 \\ a_1 & a_2 & b_0 & b_1 & b_2 \\ a_0 & a_1 & 0 & b_0 & b_1 \\ 0 & a_0 & 0 & 0 & b_0 \end{vmatrix} = 0$$
   (b) En déduire une condition nécessaire et suffisante pour que le polynôme $P = X^3 + pX + q$ de $\mathbb{K}[X]$ ait une racine multiple.
3. Pour les courageux, généraliser la question 2)a) pour m et n des entiers quelconques.

2 Polynômes irréductibles

2.1 dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$

Exercice 2.1 (Théorème de D'Alembert-Gauss)
Soit P un polynôme de degré $n \geq 1$ c'est-à-dire :

$$P = \sum_{i=0}^{n} a_i X^i$$

1. (a) Démontrer qu'il existe $R \in \mathbb{R}^+$ tel que $|P(z)| > |P(0)|$ pour tout complexe z tel que $|z| > R$.
   (b) En déduire qu'il existe un nombre complexe z_0 tel que $|P(z_0)| = \inf_{z\in\mathbb{C}} |P(z)|$.
2. On va montrer que $P(z_0) = 0$. On suppose que $P(z_0) \neq 0$ et on pose $h(X) = \dfrac{P(X+z_0)}{P(z_0)} \in \mathbb{C}[X]$, h est de degré n et on écrit $h(X) = 1 + \sum_{i=k}^{n} b_i X^i$ où $k = min\{i \in \mathbb{N}^*/b_i \neq 0\}$.
   (a) Montrer qu'il existe des nombres complexes $c_k, ..., c_n$ avec $c_k \neq 0$ tel que pour tout nombre complexe s :
   $$h(\frac{s}{c_k}) = 1 - s^k + \sum_{i=k+1}^{n} c_i s^i.$$
   (b) Montrer que pour tout $x \in]0;1[$,
   $$|\sum_{i=k+1}^{n} c_i x^{i-k}| \geq 1.$$
   (c) Conclure.

Exercice 2.2

1. Déterminer les polynômes irréductibles de $\mathbb{R}[X]$.
2. Décomposer en produit de facteurs irréductibles dans $\mathbb{R}[X]$ les polynômes suivants :
   (a) $P_1 = X^5 - 1$.
   (b) $P_2 = X^4 + X^2 - 2$.
   (c) $P_3 = X^4 - X^2 + 1$.

Exercice 2.3

1. Démontrer que le polynôme $P = 48X^4 - 32X^3 + 1$ admet une racine double réelle. Factoriser P dans $\mathbb{R}[X]$.
2. On considère le polynôme $Q = 48X^5 + 32X^4 + 20X^3 - X - 1$.
   (a) Démontrer, à l'aide de la question précédente, que Q admet une racine de la forme aj, où a est un nombre réel que l'on déterminera et où $j = e^{\frac{2i\pi}{3}}$.
   (b) Factoriser Q dans $\mathbb{R}[X]$.

2.2 dans $\mathbb{Q}[X]$

Exercice 2.4

1. Démontrer que le polynôme $X^3 + 2X^2 + X - 1$ n'admet pas de racine dans $\mathbb{Q}$. Qu'en déduit-on ?
2. A l'aide de leur décomposition en facteurs irréductibles dans $\mathbb{R}[X]$, démontrer que les polynômes suivants sont irréductibles sur $\mathbb{Q}[X]$:
   (a) $X^4 - X^2 + 1$.
   (b) $X^4 - 2$.

Exercice 2.5 (Critère d'Eisenstein)
Soit $P(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0$ un polynôme de $\mathbb{Z}[X]$ de degré n ($n \geq 1$) et p un nombre premier. On suppose que :
- p ne divise pas a_n ;
- p divise a_i pour tout $i \in \{0, ..., n-1\}$;
- p^2 ne divise pas a_0.

L'objectif de cet exercice est de montrer que P est irréductible sur $\mathbb{Q}[X]$.

1. Démontrer tout d'abord que P ne peut pas s'écrire comme produit de deux polynômes non constants dans $\mathbb{Z}[X]$.
2. Démontrer que P est irréductible sur $\mathbb{Q}[X]$ (indication : Ecrire $uvP = Q_1.R_1$ où $u, v \in \mathbb{Z}$ et $Q_1, R_1 \in \mathbb{Z}[X]$ et considérer un facteur premier p de uv et montrer que p peut être mis en facteur dans Q_1 ou dans R_1).
3. Application : démontrer que $X^n - 2$ est irréductible sur $\mathbb{Q}[X]$.

Exercice 2.6 (Polynômes cyclotomiques)
Soit n un entier supérieur ou égal à 1 ; on note $\mathbb{U}_n$ les racines n- ième de l'unité dans $\mathbb{C}$.

1. (a) Démontrer que $\mathbb{U}_n$ est un groupe (multiplicatif) cyclique d'ordre n.
   (b) On note $\mathbb{U}_n^*$ l'ensemble des racines n-ième primitives de 1. Combien en y a-t-il ?
2. On appelle n-ième polynôme cyclotomique le polynôme :

$$\Phi_n = \prod_{\zeta \in \mathbb{U}_n^*} (X - \zeta) .$$

   (a) Démontrer que pour tout entier $n \geq 1$, $X^n - 1 = \prod_{d|n} \Phi_d(X)$; en comparant les degrés quelle formule obtient-on ?
   (b) En déduire $\Phi_1, \ , \Phi_2, ..., \Phi_8$.
   (c) Démontrer que pour tout entier $n \geq 1$, $\Phi_n \in \mathbb{Z}[X]$ (raisonner par récurrence sur n).
   (d) Démontrer que pour tout nombre premier p, Φ_p est irréductible sur $\mathbb{Q}[X]$ (appliquer le critère d'Eisenstein à $\Phi_p(X + 1)$.
   Remarque : on peut montrer que $\Phi_n(X)$ est irréductible sur $\mathbb{Q}[X]$ pour tout $n \geq 1$.

3 Nombres algébriques-nombres transcendants

Définition 1
Soit $\mathbb{L}$ un corps commutatif, $\mathbb{K}$ un sous-corps de $\mathbb{L}$, $a \in \mathbb{L}$. On dit que a est algébrique sur $\mathbb{K}$ s'il existe un polynôme ***non nul*** *$P \in \mathbb{K}[X]$ tel que $P(a) = 0$ sinon on dit qu'il est transcendant. On pose $I_a = \{P \in \mathbb{K}[X]/P(a) = 0\}$ et $K[a] = \{P(a)/P \in \mathbb{K}[X]\}$*

Exemple : $\sqrt{2}$ et i sont algébriques sur $\mathbb{Q}$ car ils sont racines respectivement de $X^2 - 2$ et $X^2 + 1$.

Exercice 3.1

1. Démontrer que $\sqrt{2 + \sqrt{3}}$ est algébrique sur $\mathbb{Q}$.
2. Soit α un nombre algébrique. Démontrer qu'il existe un polynôme unitaire et irréductible de $\mathbb{Q}[X]$ non nul (appelé polynôme minimal de α sur $\mathbb{Q}$),noté P_{min} divisant tout polynôme annulant α.
3. Quel est le polynôme minimal $\sqrt[3]{2 - \sqrt{3}}$?

Exercice 3.2
Soient $\mathbb{L}$ un corps, $\mathbb{K}$ un sous-corps de $\mathbb{L}$ et $a \in \mathbb{L}$.

1. Démontrer que les propriétés suivantes sont équivalentes :
   (a) a est algébrique sur $\mathbb{K}$.
   (b) $\mathbb{K}[a]$ est un corps.
   (c) $\mathbb{K}[a]$ est un $\mathbb{K}$-espace vectoriel de dimension finie.
2. L'objectif de cette question est de démontrer que l'ensemble M des éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$ est un corps.
   (a) Démontrer que 0, 1 appartiennent à M et que si $x \in M$ et si $x \neq 0$ alors $-x$ et x^{-1} aussi.
   (b) Soit x et y des éléments de M.
      i. Démontrer que $\mathbb{K}[x; y] = \mathbb{K}[x][y]$ est un $\mathbb{K}$-espace vectoriel de dimension finie (montrer tout d'abord que c'est un $\mathbb{K}[x]$-espace vectoriel de dimension finie).
      ii. En déduire que $x + y$, $x \times y$ appartiennent à M.
   (c) Application : démontrer que $\sqrt[5]{3} - \sqrt[3]{2}$ est algébrique.

Définition 2
Un ensemble E est dénombrable s'il existe une bijection de E sur $\mathbb{N}$.

Rappels :

– Si E est dénombrable alors E^n l'est aussi pour tout $n \in \mathbb{N}$.
– Une réunion dénombrable d'ensembles dénombrables est dénombrable.

Exercice 3.3

1. Expliquer rapidement pourquoi $\mathbb{Z}$ et $\mathbb{Q}$ sont dénombrables.
2. Démontrer que $[0;1]$ n'est pas dénombrable (donc $\mathbb{R}$ aussi)(indication : raisonner par l'absurde et ranger les réels en une seule suite (x_n),pour tout entier n, écrire le développement décimal de x_n et "construire" un réel y distinct de tous les x_n).
3. Démontrer que l'ensemble des nombres algébriques sur $\mathbb{Q}$ est dénombrable (indication : on démontera tout d'abord que l'ensemble $\mathbb{Q}_n[X]$ des polynômes nul ou de degré inférieur à n ($n \geq 1$) est dénombrable). Qu'en déduit-on ?

Exercice 3.4 (Nombre de Liouville)

1. Soient α un nombre algébrique, n le degré du polynôme P_{min} minimal annulant α.
   (a) Démontrer Tout d'abord que pour tout
   $$(p;q) \in \mathbb{Z} \times \mathbb{N}^* |P_{min}\left(\frac{p}{q}\right)| \geq \frac{1}{q^n}$$
   (b) Démontrer qu'il existe un réel positif k tel que :
   $$\forall (p;q) \in \mathbb{Z} \times \mathbb{N}^*,\ 0 < |\alpha - \frac{p}{q}| < 1 \Rightarrow |\alpha - \frac{p}{q}| > \frac{k}{q^n}$$
   (indication : appliquer le théorème des accroissements finis).
2. En déduire que $\alpha = \sum_{i=1}^{+\infty} \frac{1}{10^{i!}}$ est transcendant.