Exercices de khôlle pour la MPSI

Treizième semaine

David A. Madore

david.madore@clipper.ens.fr

http://www.eleves.ens.fr:8080/home/madore/index.html

(Jusqu'à présent : Moyenne des notes : 14.66 ± 0.33. Écart type : 2.77.

Théorème de Fermat sur les polynômes. *Montrer que si $n \geq 3$, l'équation $x^n + y^n = z^n$ n'a pas de solution dans $\mathbb{C}[X]$ avec x, y, z tous non nuls.*

> **Indication :** Montrer qu'on peut supposer x, y, z sans facteurs communs. Dériver la relation et la multiplier par z. Conclure par une considération de degré.

Problème "de Waring facile". *Waring a conjecturé, et Hilbert a démontré, que pour tout naturel n il existe un naturel $r(n)$ tel que tout naturel s'écrive comme somme de au plus $r(n)$ puissances n-ièmes de naturels. Nous nous proposons de démontrer le résultat plus faible suivant : pour tout naturel n il existe un naturel $r(n)$ tel que tout naturel s'écrive comme somme ou différence de au plus $r(n)$ puissances n-ièmes de naturels. En fait, on va montrer un résultat un peu plus général.*

(i) Si $P \in \mathbb{Z}[X]$ est un polynome à coefficients entiers, montrer que ΔP défini par $\Delta P(X) = P(X+1) - P(X)$ est un polynôme à coefficients entiers, et que, si $\deg P > 0$, alors $\deg \Delta P = \deg P - 1$.

(ii) Montrer que pour tout polynôme $P \in \mathbb{Z}[X]$ prenant les valeurs 0 et 1 sur des naturels il existe un naturel $r(P)$ tel que tout naturel s'écrive comme somme ou différence de au plus $r(P)$ valeurs de P sur des naturels (i.e. pour tout $a \in \mathbb{N}$ il existe $a_1, \ldots, a_k$ naturels avec $k \leq r(P)$, et $\varepsilon_1, \ldots, \varepsilon_k \in \{-1, +1\}$ tels que $a = \varepsilon_1 P(a_1) + \cdots + \varepsilon_k P(a_k)$). (Indication : considérer $\Delta^{q-1} P$ où $q = \deg P$.)

Polynômes cyclotomiques. *On rappelle qu'on dit qu'un entier d divise un entier n (notation $d|n$) ss'il existe $q \in \mathbb{Z}$ tel que $n = qd$, et que deux entiers k et n sont premiers entre eux ssi les seuls entiers qui divisent k et n sont 1 et -1. On définit le n-ième polynôme cyclotomique comme $\Phi_n(X) = \prod_k (X - e^{2ik\pi/n})$, où k décrit l'ensemble des entiers entre 0 et $n-1$ et premiers avec n. Montrer que*

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

et en déduire par récurrence sur n que Φ_n est à coefficients entiers.

Introduction à la théorie de Galois. *Soit K un corps tel que $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$; on appelle <u>groupe de Galois</u> G de K sur $\mathbb{Q}$ le groupe de tous les morphismes bijectifs de K sur lui-même qui sont l'identité sur $\mathbb{Q}$. Soit $P \in \mathbb{Q}[X]$ un polynôme à coefficients rationnels, dont toutes les racines complexes sont en fait dans K ; on suppose de plus que si α, α' sont deux racines (complexes) de P il existe $\sigma \in G$ tel que $\alpha' = \sigma(\alpha)$ (on dit que G opère transitivement sur l'ensemble des racines complexes de P). Montrer que P est irréductible sur $\mathbb{Q}[X]$.*

Un super-grand-classique. *On appelle nombre algébrique (sur $\mathbb{Q}$) un nombre complexe qui est racine d'un polynôme de $\mathbb{Q}[X]$, et on appelle $\bar{\mathbb{Q}}$ l'ensemble des nombres algébriques (sur $\mathbb{Q}$).*

(i) Montrer que $\bar{\mathbb{Q}}$ est un corps.

(ii) Montrer que tout polynôme non constant de $\bar{\mathbb{Q}}[X]$ est scindé (i.e. $\bar{\mathbb{Q}}$ est algébriquement clos).

Exercice inqualifié. *Montrer que les polynômes suivants sont irréductibles dans $\mathbb{Q}[X]$: X^2+1, X^2+X+1, X^2+2X+2, X^3+2X+2, X^4+2X+2, $X^4+5X^3+10X^2+10X+5$, $X^4+X^3+X^2+X+1$.*

Exercice trivial. *Montrer que les fonctions suivantes ne sont pas des polynômes :* $x \mapsto e^x$, $x \mapsto \cos x$, $x \mapsto \sqrt{x^2+1}$.

Corps de rupture. *Soit* K *un corps, et* $P \in K[X]$ *de degré* $d \geq 2$. *On appelle* L *le* K*-espace vectoriel des polynômes de* $K[X]$ *de degré strictement inférieur à* d. *On munit* L *d'une multiplication* $\star$ *de la manière suivante : si* $x, y \in L$, *alors* $x \star y$ *est le reste de la division euclidienne de* xy *par* P. *Montrer que cette multiplication donne à* L *une structure de* K*-algèbre, et que cette* K*-algèbre est un corps ssi* P *est irréductible. Montrer de plus que, dans ce cas,* P *admet une racine dans* L.

Anneau des séries formelles. *On appelle* <u>*série formelle*</u> *à coefficients dans un corps* K *une suite* $(P_i)_{i\in\mathbb{N}}$ *d'éléments de* $K[X]$ *telle que pour tout* i, P_i *soit de degré au plus* i, *et* $P_{i+1} - P_i$ *de valuation au moins* $i+1$. *On note* $K[[X]]$ *l'ensemble des séries formelles à coefficients dans* K. *On définit deux opérations* $+$ *et* $\times$ *sur* $K[[X]]$ *par* $(P_i) + (Q_i) = (P_i + Q_i)$ *et* $(P_i) \times (Q_i) = (R_i)$ *où* R_i *est le reste de la division euclidienne de* P_iQ_i *par* X^{i+1}. *Montrer qu'elles font de* $K[[X]]$ *un anneau intègre.*

Idéaux de $K[X]$. *On appelle* <u>*idéal*</u> *de* $K[X]$ *un sous-groupe additif* $\mathfrak{i}$ *de* $K[X]$ *tel que* $AP \in \mathfrak{i}$ *dès que* $A \in K[X]$ *et* $P \in \mathfrak{i}$. *Montrer que si* $P \in K[X]$ *alors l'ensemble* $(P) = \{PQ : Q \in K[X]\}$ *est un idéal de* $K[X]$ *; un tel idéal est dit* <u>*principal*</u>. *Montrer que tout idéal de* $K[X]$ *est principal (on dit que* $K[X]$ *est un anneau principal).*

Lemme des noyaux. *Soient* $P, Q \in \mathbb{C}[X]$ *deux polynômes premiers entre eux, et* u *un endomorphisme d'un* $\mathbb{C}$*-espace vectoriel* E *(i.e.* u *est une application linéaire de* E *dans* E*). Montrer que*

$$\ker PQ(u) = \ker P(u) \oplus \ker Q(u)$$

Autre grand classique. *Soit* $P \in \mathbb{R}[X]$ *tel que* $P(-x) = P(x)$ *pour tout* x. *Montrer que* P *n'a que des monômes de degré pair.*