MPSI 2

Programme des colles de mathématiques.

Semaine 23 : du lundi 13 avril au vendredi 18.

Les polynômes

Liste des questions de cours

1°) Enoncer et démontrer une propriété portant sur le degré de la composée de deux polynômes.

2°) Enoncer et démontrer le théorème d'existence et d'unicité de la division euclidienne entre polynômes.

3°) Montrer que a est racine de P si et seulement si $(X-a) \mid P$.

4°) Montrer que $\mathbb{K}[X]$ est un anneau principal.

5°) Montrer qu'un polynôme de degré 2 ou 3 est irréductible dans $\mathbb{K}[X]$ si et seulement si il ne possède aucune racine dans $\mathbb{K}$.

6°) Dans $\mathbb{K}[X]$, énoncer et démontrer le théorème d'existence et unicité de la décomposition d'un polynôme en produit de polynômes d'irréductibles.

7°) Ecrire (en justifiant) tout polynôme $P \in \mathbb{K}_n[X]$ en fonction des polynômes d'interpolation de Lagrange associés à une famille de $n+1$ scalaires deux à deux distincts.

8°) Enoncer et démontrer la formule de Taylor.

9°) Enoncer et démontrer une propriété qui fait le lien entre multiplicité de a pour P et dérivées successives de P en a.

10°) Soit $P(X) = X^3+aX^2+bX+c \in \mathbb{K}[X]$ un polynôme scindé dans $\mathbb{K}[X]$, dont les racines, comptées avec multiplicité sont notées x_1, x_2 et x_3. Calculer $S = \dfrac{1}{x_1+1} + \dfrac{1}{x_2+1} + \dfrac{1}{x_3+1}$ en fonction de a, b, c.

11°) Lorsque $P \in \mathbb{C}[X]$, montrer que α est racine de P de multiplicité m si et seulement si $\overline{\alpha}$ est racine de $\overline{P}$ de multiplicité m.

Les polynômes

1 L'anneau des polynômes

Notation. A désigne un anneau quelconque.

Polynômes formels de $A[X]$. Addition entre polynômes. $(A[X], +)$ est un groupe.

Degré d'un polynôme. $A[X] = \displaystyle\bigcup_{n\in\mathbb{N}} A_n[X]$.

Degré d'une somme de polynômes.

Produits de polynômes. $(A[X], +, \times)$ est un anneau contenant A.

$A[X]$ est commutatif intègre si et seulement si A est commutatif intègre.

Pour toute la suite, on suppose que A est commutatif intègre.

Degré d'un produit de polynômes.

Ensemble des polynômes inversibles.

Application polynomiale $\tilde{P} \in A^A$ associée à un polynôme formel $P \in A[X]$.
$P \longmapsto \tilde{P}$ est un morphisme d'anneaux.

Algorithme d'Hörner.

Définition de $A[X_1, \ldots, X_n]$: aucune connaissance n'est exigible sur les polynômes à plusieurs indéterminées.

Composition de polynômes.
Si $\deg(Q) \geq 1$, alors $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Dérivation formelle. Dérivée d'ordre n.
$\deg(P') \leq \deg(P) - 1$: **Le cas d'égalité est précisé plus loin.**
Dérivée d'une combinaison linéaire, d'un produit, formule de Leibniz, dérivée d'une composée.

Pour la suite, $\mathbb{K}$ désigne un corps.

Division euclidienne.
Reste de la division de P par $X - a$. a est racine de P si et seulement si $(X - a)|P$.
Si $\mathbb{L}$ est un sous-corps de $\mathbb{K}$, les quotient et reste de la division euclidienne de $A \in \mathbb{L}[X]$ par $B \in \mathbb{L}[X] \setminus \{0\}$ sont les mêmes que l'on regarde A et B comme des polynômes de $\mathbb{L}[X]$ ou de $\mathbb{K}[X]$.

2 Arithmétique

2.1 Divisibilité dans un anneau commutatif A

$a|b \iff bA \subseteq aA$.
La relation de divisibilité est réflexive et transitive.
Eléments de A associés.

Hypothèse : on suppose que A est un anneau intègre.

Soit $a, b \in A$. a et b sont associés si et seulement s'il existe $\lambda \in U(A)$ tel que $a = \lambda b$.
La relation de divisibilité est un ordre sur $\mathbb{N}$ et sur l'ensemble des polynômes unitaires de $\mathbb{K}[X]$.

Eléments irréductibles de A.

Eléments de A premiers entre eux, deux à deux ou globalement.

Si $p \in A$ est irréductible, pour tout $a \in A$, $p|a$, ou bien p et a sont premiers entre eux.

2.2 PGCD et PPCM

$\mathbb{K}[X]$ est un anneau principal.

Notation. Dans ce chapitre, A désigne un anneau principal.
PGCD et PPCM de deux éléments : définition par idéaux, caractérisation par divisibilité.
PGCD et PPCM de k éléments, d'une partie quelconque de A.

Commutativité et associativité des PGCD et PPCM,
distributivité du produit par rapport au PGCD et au PPCM.

2.3 Bezout et Gauss

Identité de Bezout, théorème de Gauss.
Si $p \mid ab$ avec p irréductible, alors $p \mid a$ ou $p \mid b$.

Si $a \wedge b = a \wedge c = 1$, alors $a \wedge bc = 1$.
Si $a|b$, $c|b$ et $a \wedge c = 1$ alors $ac|b$.
ab et $(a \wedge b)(a \vee b)$ sont associés.

2.4 $\mathbb{Z}$ et $\mathbb{K}[X]$ sont factoriels

Notation. Ici, $A = \mathbb{Z}$ ou $A = \mathbb{K}[X]$. Si $A = \mathbb{Z}$, $\mathcal{P}$ désigne $\mathbb{P}$, et si $A = \mathbb{K}[X]$, $\mathcal{P}$ est l'ensemble des polynômes irréductibles et unitaires.

Existence et unicité de la décomposition en produit d'irréductibles.
Si $a = u \prod\limits_{p \in \mathcal{P}} p^{\nu_p}$ et $b = v \prod\limits_{p \in \mathcal{P}} p^{\mu_p}$, alors $a \mid b \iff [\forall p \in \mathcal{P},\ \nu_p \leq \mu_p]$,
$a \wedge b = \prod\limits_{p \in \mathcal{P}} p^{\min(\nu_p, \mu_p)}$ et $a \vee b = \prod\limits_{p \in \mathcal{P}} p^{\max(\nu_p, \mu_p)}$.

2.5 Algorithme d'Euclide

Lemme d'Euclide : si $a = bq + r$, alors $a \wedge b = b \wedge r$.
Algorithme d'Euclide. Utilisation de l'algorithme d'Euclide pour calculer des coefficients de Bezout de deux polynômes (ou de deux entiers) premiers entre eux.

En exercice : pour $a, b \in A$, solutions de l'équation de Bézout $(B)\ :\ au + bv = c$ en l'inconnue $(u, v) \in A^2$.

Si $\mathbb{L}$ est un sous-corps de $\mathbb{K}$ et $(A, B) \in \mathbb{L}[X] \times (\mathbb{L}[X] \setminus \{0\})$, les PGCD et PPCM de A et B sont les mêmes, que l'on regarde A et B comme des polynômes de $\mathbb{L}[X]$ ou de $\mathbb{K}[X]$.

3 Racines d'un polynôme

3.1 Identification entre polynômes formels et applications polynomiales

$a_1, \ldots, a_k$ sont racines de P si et seulement si P est un multiple de $(X - a_1) \times \cdots \times (X - a_k)$.
Un polynôme non nul admet au plus $\deg(P)$ racines.

Principe de rigidité des polynômes : si $P \in \mathbb{K}[X]$ possède une infinité de racines, alors $P = 0$.
Lorsque $P, Q \in \mathbb{K}_n[X]$, si $\{x \in \mathbb{K} \ / \ \tilde{P}(x) = \tilde{Q}(x)\}$ contient au moins $n + 1$ scalaires, alors $P = Q$.

Identification entre polynômes formels et applications polynomiales de $\mathbb{K}$ dans $\mathbb{K}$ lorsque $\mathbb{K}$ est infini.

Polynômes d'interpolation de Lagrange.

3.2 Polynôme dérivé, lorsque car$(\mathbb{K}) = 0$

$\deg(P) \geq 1 \Longrightarrow \deg(P') = \deg(P) - 1$.

Formule de Taylor. Reste de la division euclidienne par $(X - a)^k$.

3.3 Racines multiples

Racine de multiplicité au moins m de P ou exactement m de P.

Les a_h sont racines de P de multiplicité au moins m_h si et seulement si $\prod\limits_{h=1}^{k} (X - a_h)^{m_h}$ divise P.

Le nombre de racines de P (non nul), comptées avec multiplicité est inférieur ou égal au degré de P.

Lorsque car$(\mathbb{K}) = 0$, lien entre multiplicité de a et dérivées successives en a.

3.4 Polynômes scindés

Polynômes scindés, simplement scindés.

Relations de Viète entre coefficients et racines.

3.5 Polynômes de $\mathbb{R}[X]$ et de $\mathbb{C}[X]$

$\begin{array}{rcl} \mathbb{C}[X] & \longrightarrow & \mathbb{C}[X] \\ P & \longmapsto & \overline{P} \end{array}$ est un isomorphisme d'anneaux.

α est racine de P de multiplicité m si et seulement si $\overline{\alpha}$ est racine de $\overline{P}$ de multiplicité m.

Théorème de d'Alembert.
Dans $\mathbb{C}[X]$, le nombre de racines avec multiplicité, de tout polynôme non nul est égal à son degré.
$P \mid Q$ si et seulement si toute racine de P est racine de Q avec une multiplicité pour Q supérieure ou égale à celle pour P.

Polynômes irréductibles de $\mathbb{R}[X]$.

Prévisions pour la semaine suivante :

Fractions rationnelles.