Semaine 14

du 22 au 26 janvier 2024

▶ Arithmétique sur $\mathbb{Z}$ et $\mathbb{K}[X]$

➠ ***Reprise du programme de la semaine 10.***

- notion de polynôme à une indéterminée sur un corps $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$, structure d'anneau intègre sur $\mathbb{K}[X]$, inversibles ;
- composition de polynômes ;
- degré d'un polynôme (appartenant à $\mathbb{N} \cup \{-\infty\}$), notion de polynôme constant, de coefficient dominant, de polynôme unitaire ;
- degré d'une somme, d'un produit, d'une composée de polynômes ;
- polynômes multiples, diviseurs d'un autre polynôme, relation "|" sur $\mathbb{K}[X]$;
- division euclidienne sur $\mathbb{K}[X]$;
- un pgcd de deux polynômes A et B est par convention tout élément de degré maximal divisant A et B : ils sont tous associés et il existe un unique tel polynôme unitaire, noté $A \wedge B$ ou $\text{pgcd}(A, B)$;
- algorithme d'Euclide sur $\mathbb{K}[X]$;
- théorèmes de Bézout et Gauss ;
- notion de ppcm, unicité dans le cas unitaire, formule $\frac{AB}{\text{cd(AB)}} = (A \wedge B)(A \vee B)$;
- l'ensemble $\mathbb{K}[x]$ des fonctions polynomiales sur $\mathbb{K}$ est en bijection avec $\mathbb{K}[X]$;
- évaluation d'un polynôme P en un point a via sa fonction polynomiale associée, notation (abusive) $P(a)$;
- racines d'un polynôme, tout polynôme admet au plus un nombre de racines égal à son degré ;
- $a \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ si et seulement si $X - a$ divise P.

✖ ***Aucune connaissance n'est exigible des étudiant·e·s sur les sujets suivants : construction de*** $\mathbb{K}[X]$***, polynômes sur un corps fini, dérivation des polynômes, racines multiples, formule de Taylor, polynômes irréductibles, théorème de d'Alembert–Gauss, crypto–systèmes RSA, indicatrice d'Euler, anneaux*** $\mathbb{Z}/n\mathbb{Z}$***.***

▶ Questions de cours (*démonstrations*)

- tout énoncé ou définition est exigible ;
- division euclidienne sur $\mathbb{K}[X]$;
- lemme de Gauss (sur $\mathbb{Z}$ ou $\mathbb{K}[X]$) ;
- si p est premier et $a, b \in \mathbb{Z}$, $(a+b)^p \equiv a^p + b^p \,[p]$, petit théorème de Fermat ;
- $a \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ si et seulement si $X - a$ divise P.

♦ Exercices CCINP : 86, 94.