Colle de mathématiques n° 18
MP*1 & MP*2
Semaine du 02 au 07 mars 2020

Au programme cette semaine :
– arithmétique des anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ vue sous l'angle de la structure de leurs idéaux,
– étude des congruences dans $\mathbb{Z}$ à l'aide de la structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$,
– fin des probabilités.

Structures algébriques usuelles

CONTENUS	CAPACITÉS & COMMENTAIRES
e) Anneaux	
Anneau. Produit fini d'anneaux. Sous-anneaux. Morphisme d'anneaux. Image et noyau d'un morphisme. Isomorphisme d'anneaux.	Les anneaux sont unitaires.
Anneau intègre. Corps. Sous-corps.	Les corps sont commutatifs.
f) Idéaux d'un anneau commutatif	
Idéal d'un anneau commutatif. Le noyau d'un morphisme d'anneaux est un idéal. Relation de divisibilité dans un anneau commutatif intègre. Idéaux de $\mathbb{Z}$.	Interprétation de la divisibilité en termes d'idéaux.
g) L'anneau $\mathbb{Z}/n\mathbb{Z}$	
Anneau $\mathbb{Z}/n\mathbb{Z}$. Inversibles de $\mathbb{Z}/n\mathbb{Z}$.	L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
Théorème chinois : si m et n sont deux entiers premiers entre eux, isomorphisme naturel de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.	Application aux systèmes de congruences.
Indicatrice d'Euler φ. Calcul de $\varphi(n)$ à l'aide de la décomposition de n en facteurs premiers.	$\leftrightarrows$ I : calcul de $\varphi(n)$ à l'aide d'une méthode de crible.
Théorème d'Euler.	Lien avec le petit théorème de Fermat étudié en première année. $\leftrightarrows$ I : codage RSA.
h) Anneaux de polynômes à une indéterminée	
Dans ce paragraphe, K est un sous-corps de $\mathbb{C}$.	
Idéaux de $K[X]$. PGCD de deux polynômes.	Par convention, le PGCD est unitaire. Extension au cas d'une famille finie.
Relation de Bézout. Lemme de Gauss.	$\leftrightarrows$ I : algorithme d'Euclide étendu sur les polynômes, recherche simultanée du PGCD et des coefficients de Bézout.

CONTENUS	CAPACITÉS & COMMENTAIRES
Irréductible de $K[X]$. Existence et unicité de la décomposition en facteurs irréductibles.	Les étudiants doivent connaître les irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$. L'étude des polynômes sur un corps fini est hors programme.

Variables aléatoires discrètes

CONTENUS	CAPACITÉS & COMMENTAIRES
i) Loi faible des grands nombres	
Si $(X_n)_{n\geqslant 0}$ est une suite de variables aléatoires deux à deux indépendantes, de même loi et admettant un moment d'ordre 2, alors, si $S_n = \sum_{k=1}^{n} X_k$ et $m = \mathrm{E}(X_1)$, on a, $$P\left(\left\lvert \frac{S_n}{n} - m\right\rvert \geqslant \varepsilon\right) \underset{n\to+\infty}{\longrightarrow} 0.$$	Les étudiants doivent savoir retrouver, pour $\varepsilon > 0$, l'inégalité : $$P\left(\left\lvert \frac{S_n}{n} - m\right\rvert \geqslant \varepsilon\right) \leqslant \frac{\sigma^2}{n\varepsilon^2}$$ où σ est la variance commune des X_k. $\leftrightarrows$ I : simulation d'une suite de tirages.
j) Fonctions génératrices	
Fonction génératrice de la variable aléatoire X à valeurs dans $\mathbb{N}$: $$G_X(t) = \mathrm{E}(t^X) = \sum_{k=0}^{+\infty} P(X=k)\, t^k.$$	La série entière définissant G_X est de rayon supérieur ou égal à 1 et converge normalement sur le disque fermé de centre 0 et de rayon 1. Continuité de G_X.
Détermination de la loi de X par G_X. Utilisation de G_X pour calculer les moments de X. La variable aléatoire X est d'espérance finie si et seulement si G_X est dérivable en 1 ; dans ce cas $\mathrm{E}(X) = {G_X}'(1)$. La variable aléatoire X admet un second moment si et seulement si G_X est deux fois dérivable en 1.	Les étudiants doivent savoir retrouver l'expression de la variance de X à l'aide de ${G_X}'(1)$ et ${G_X}''(1)$. Les étudiants doivent savoir calculer la fonction génératrice d'une variable aléatoire de Bernoulli, binomiale, géométrique, de Poisson.
Fonction génératrice d'une somme finie de variables aléatoires indépendantes à valeurs dans $\mathbb{N}$.	