



Colle de mathématiques n° 18
MP*1 & MP*2
Semaine du 27 février au 04 mars 2017

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.
Anneau intègre. Corps. Sous-corps.

Les anneaux sont unitaires.

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 $\mathbb{Z}/n\mathbb{Z}$.

Théorème chinois : si m et n sont deux entiers premiers entre eux, isomorphisme naturel de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
Indicatrice d'Euler φ . Calcul de $\varphi(n)$ à l'aide de la décomposition de n en facteurs premiers.
Théorème d'Euler.

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
Application aux systèmes de congruences.

 \Leftrightarrow I : calcul de $\varphi(n)$ à l'aide d'une méthode de crible.

Lien avec le petit théorème de Fermat étudié en première année.
 \Leftrightarrow 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.

Relation de Bézout. Lemme de Gauss.

Irréductible de $K[X]$. Existence et unicité de la décomposition en facteurs irréductibles.

Par convention, le PGCD est unitaire.
Extension au cas d'une famille finie.
 \Leftrightarrow I : algorithme d'Euclide étendu sur les polynômes, recherche simultanée du PGCD et des coefficients de Bézout.
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

Programme précédent plus

CONTENUS

CAPACITÉS & COMMENTAIRES

i) Loi faible des grands nombres

Si $(X_n)_{n \geq 0}$ 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 $m = E(X_1)$, on a,

$$P\left(\left|\frac{S_n}{n} - m\right| \geq \varepsilon\right) \xrightarrow{n \rightarrow +\infty} 0.$$

Les étudiants doivent savoir retrouver, pour $\varepsilon > 0$, l'inégalité :

$$P\left(\left|\frac{S_n}{n} - m\right| \geq \varepsilon\right) \leq \frac{\sigma^2}{n\varepsilon^2}$$

où σ est la variance commune des X_k .
 \Leftrightarrow I : simulation d'une suite de tirages.

j) Fonctions génératrices

Fonction génératrice de la variable aléatoire X à valeurs dans \mathbb{N} :

$$G_X(t) = E(t^X) = \sum_{k=0}^{+\infty} P(X = k) t^k.$$

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 $E(X) = G_X'(1)$. La variable aléatoire X admet un second moment si et seulement si G_X est deux fois dérivable en 1.

Fonction génératrice d'une somme finie de variables aléatoires indépendantes à valeurs dans \mathbb{N} .

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 .

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.