Colle de mathématiques n° 18
MP*1 & MP*2
Semaine du 05 au 10 mars 2018

Structures algébriques usuelles

Programme précédent plus :

CONTENUS	CAPACITÉS & COMMENTAIRES
a) Groupes et sous-groupes	
Groupe. Produit fini de groupes. Sous-groupe. Caractérisation. Intersection de sous-groupes. Sous-groupe engendré par une partie. Sous-groupes du groupe $(\mathbb{Z},+)$.	Exemples issus de l'algèbre et de la géométrie.
b) Morphismes de groupes	
Morphisme de groupes. Image et image réciproque d'un sous-groupe par un morphisme. Image et noyau d'un morphisme. Condition d'injectivité d'un morphisme. Isomorphisme de groupes. Réciproque d'un isomorphisme.	Exemples : signature, déterminant. Exemple : groupe spécial orthogonal d'un espace euclidien.
c) Groupes monogènes et cycliques	
Groupe $(\mathbb{Z}/n\mathbb{Z},+)$. Générateurs de $\mathbb{Z}/n\mathbb{Z}$. Groupe monogène, groupe cyclique. Tout groupe monogène infini est isomorphe à $(\mathbb{Z},+)$. Tout groupe monogène fini de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.	Groupe des racines n-ièmes de l'unité.
d) Ordre d'un élément dans un groupe	
Élément d'ordre fini d'un groupe, ordre d'un tel élément. Si x est d'ordre fini d et si e désigne le neutre de G, alors, pour n dans $\mathbb{Z}$, on a $x^n = e \iff d \mid n$. L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.	Si x est d'ordre fini, l'ordre de x est le cardinal du sous-groupe de G engendré par x. La démonstration n'est exigible que pour G commutatif.

CONTENUS	CAPACITÉS & COMMENTAIRES
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.

CONTENUS	CAPACITÉS & COMMENTAIRES
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.
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.