Exercices

Ils porteront sur les notions de ce chapitre

Cours

Structures algébriques usuelles

L'étude des structures algébriques offre l'occasion d'approfondir plusieurs points abordés en première année : arithmétique de $\mathbb{Z}$ et de $\mathbb{K}[X]$, congruences, algèbre linéaire, groupe symétrique, groupes issus de l'algèbre linéaire, ou, ultérieurement, de la géométrie des espaces euclidiens.

Le paragraphe relatif aux polynômes permet de revenir sur l'étude menée en première année, dans un cadre étendu et dans un esprit plus algébrique mettant l'accent sur la notion d'idéal.

CONTENUS	CAPACITÉS & COMMENTAIRES
a) Compléments sur les groupes	
Intersection de sous-groupes. Sous-groupe engendré par une partie. Partie génératrice d'un groupe. Sous-groupes du groupe $(\mathbb{Z},+)$. $(\star)$ Groupe $(\mathbb{Z}/n\mathbb{Z},+)$. Générateurs de $\mathbb{Z}/n\mathbb{Z}$.	
Groupe monogène, groupe cyclique.	Groupe des racines n-ièmes de l'unité.
Tout groupe monogène infini est isomorphe à $(\mathbb{Z},+)$. Tout groupe monogène fini de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.	
Ordre d'un élément d'un groupe.	L'ordre de x est le cardinal du sous-groupe de G engendré par x.
Si x est d'ordre fini d et si e désigne le neutre de G, alors, pour tout $n\in\mathbb{Z}$, $x^n=e \iff d\|n$.	
$(\star)$ L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.	La démonstration n'est exigible que pour G commutatif.
b) Compléments sur les anneaux	
Produit fini d'anneaux.	
Idéal d'un anneau commutatif.	Noyau d'un morphisme d'anneaux commutatifs.
Idéal engendré par un élément.	Notation xA.
Divisibilité dans un anneau commutatif intègre.	Interprétation en termes d'idéaux.
c) Idéaux de $\mathbb{Z}$	
Idéaux de $\mathbb{Z}$.	
Définition du PGCD de $n\geqslant 2$ entiers relatifs en termes d'idéaux, relation de Bézout.	Lien avec le programme de première année.
d) Anneaux $\mathbb{Z}/n\mathbb{Z}$	
Anneau $\mathbb{Z}/n\mathbb{Z}$.	
$(\star)$ Inversibles de $\mathbb{Z}/n\mathbb{Z}$. $(\star)$ Condition nécessaire et suffisante pour que $\mathbb{Z}/n\mathbb{Z}$ soit un corps.	Notation $\mathbb{F}_p$ lorsque p est premier.
$(\star)$ Théorème chinois : isomorphisme naturel de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ si $m\wedge n=1$; extension à plus de deux facteurs.	$(\star)$ Application aux systèmes de congruences et à la résolution de systèmes d'équations dans $\mathbb{Z}/n\mathbb{Z}$.
$(\star)$ Indicatrice d'Euler φ. $(\star)$ Calcul à l'aide de la décomposition en produits de facteurs premiers.	$(\star)$Relation $\varphi(mn)=\varphi(m)\varphi(n)$ si m et n sont premiers entre eux ; expression de $\varphi(p^k)$ pour p premier.

Contenus	Capacités & Commentaires
($\star$) Théorème d'Euler.	Lien avec le petit théorème de Fermat.

e) Anneaux $\mathbb{K}[X]$

Dans ce paragraphe, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.	
($\star$) Idéaux de $\mathbb{K}[X]$.	
Définition du PGCD de $n \geqslant 2$ polynômes en termes d'idéaux, relation de Bézout.	Par convention, le PGCD est unitaire.
Irréductibles de $\mathbb{K}[X]$. Existence et unicité de la décomposition en facteurs irréductibles unitaires.	
($\star$) Irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$.	La démonstration du théorème de d'Alembert-Gauss est hors programme. L'étude des irréductibles de $\mathbb{K}[X]$ pour un corps autre que $\mathbb{R}$ ou $\mathbb{C}$ n'est pas un objectif du programme.

f) Algèbres

Les définitions doivent etre connues. Algèbre. Sous-algèbre. Morphisme d'algèbres.	Les algèbres sont unitaires. Exemples : $\mathbb{K}[X]$, $\mathscr{L}(E)$, $\mathscr{M}_n(\mathbb{K})$, $\mathscr{F}(X,\mathbb{K})$.