Structures algébriques usuelles

L'étude des structures algébriques permet 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 et de la géométrie des espaces euclidiens. Ce chapitre gagne à être illustré par de nombreux exemples.
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.
Sans soulever de difficulté, on signalera que les notions d'algèbre linéaire étudiées en MPSI s'étendent au cas où le corps de base est un sous-corps de $\mathbb{C}$.

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

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.

⇆ 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.

⇆ 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.

⇆ 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.

i) Algèbres

Algèbre.

Les algèbres sont unitaires.

Exemples : $\mathbb{K}[X]$, $\mathcal{L}(E)$, $\mathcal{M}_n(\mathbb{K})$, $\mathcal{F}(X, \mathbb{K})$.

Sous-algèbre.

Morphisme d'algèbres.