

Programme

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 $(\mathbb{Z}, +)$.

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 $(\mathbb{Z}/n\mathbb{Z}, +)$.

Ordre d'un élément d'un groupe.

Si x est d'ordre fini d et si e désigne le neutre de G , alors, pour tout $n \in \mathbb{Z}$, $x^n = e \iff d|n$.

L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.

Groupe des racines n -ièmes de l'unité.

L'ordre de x est le cardinal du sous-groupe de G engendré par x .

La démonstration n'est exigible que pour G commutatif.

b) Compléments sur les anneaux

Produit fini d'anneaux.

Idéal d'un anneau commutatif.

Idéal engendré par un élément.

Divisibilité dans un anneau commutatif intègre.

Noyau d'un morphisme d'anneaux commutatifs.

Notation xA .

Interprétation en termes d'idéaux.

c) Idéaux de \mathbb{Z}

Idéaux de \mathbb{Z} .

Définition du PGCD de $n \geq 2$ entiers relatifs en termes d'idéaux, relation de Bézout.

Lien avec le programme de première année.

d) Anneaux $\mathbb{Z}/n\mathbb{Z}$ (non traité)

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

Inversibles de $\mathbb{Z}/n\mathbb{Z}$. Condition nécessaire et suffisante pour que $\mathbb{Z}/n\mathbb{Z}$ soit un corps.

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.

Indicatrice d'Euler φ . Calcul à l'aide de la décomposition en produits de facteurs premiers.

Théorème d'Euler.

Notation \mathbb{F}_p lorsque p est premier.

Application aux systèmes de congruences et à la résolution de systèmes d'équations dans $\mathbb{Z}/n\mathbb{Z}$.

Relation $\varphi(mn) = \varphi(m)\varphi(n)$ si m et n sont premiers entre eux; expression de $\varphi(p^k)$ pour p premier.

Lien avec le petit théorème de Fermat.

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

Dans ce paragraphe, \mathbb{K} est un sous-corps de \mathbb{C} .

Idéaux de $\mathbb{K}[X]$.

Définition du PGCD de $n \geq 2$ polynômes en termes d'idéaux, relation de Bézout.

Irréductibles de $\mathbb{K}[X]$. Existence et unicité de la décomposition en facteurs irréductibles unitaires.

Par convention, le PGCD est unitaire.