

# Structure algébrique et arithmétique



## En bref

- > **Langues d'enseignement:** Français
- > **Ouvert aux étudiants en échange:** Oui

## Présentation

### Description

Cardinalités. Généralités sur les structures de groupe, anneau, corps. Application à l'arithmétique.

### Objectifs

Introduire et étudier les structures de base de l'algèbre : groupes, anneaux et corps.

Appliquer ces outils à l'arithmétique.

### Heures d'enseignement

Structure algébrique et arithmétique - CM	Cours Magistral	22,5h
Structure algébrique et arithmétique - TD	Travaux Dirigés	27h
Structure algébrique et arithmétique - [EFA] CM	Cours magistral - Enseignement favorisant l'autonomie	1,5h
Structure algébrique et arithmétique - [EFA] TD	Travaux dirigés - Enseignement favorisant l'autonomie	3h

### Pré-requis obligatoires

Enseignements d'algèbre de première année.

---

## Plan du cours

**Cardinalité.** Ensembles finis, ensembles dénombrables, théorème de Cantor, puissance du continu.

**Structures algébriques et structures quotient.**

**Groupes.** Groupes, sous-groupes, morphismes, noyau, ordre d'un élément, groupe monogène, groupe cyclique, quotient d'un groupe commutatif, indice d'un sous-groupe, théorème de Lagrange. Exemples : Groupe cyclique  $\mathbf{Z}/n\mathbf{Z}$ , groupe symétrique  $S_n$  (générateurs et groupes alternés  $A_n$ ) et sous-groupes de  $(\mathbf{R}, +)$ .

**Anneaux.** Anneaux, sous-anneaux, morphismes, idéaux, quotient d'un anneau par un idéal, idéaux premiers et maximaux et introduction élémentaire à la structure de corps (corps et morphismes de corps).

**Algèbres.** Structure d'algèbre, polynômes en plusieurs indéterminées sur un corps, polynômes symétriques, séries formelles et exemples d'algèbres de fonctions venant de l'analyse.

**Arithmétique des entiers & des polynômes.** Quotients de  $\mathbf{Z}$ , divisibilité, ppcm, pgcd, éléments premiers, éléments irréductibles, les nombres premiers forment un ensemble infini, énoncé du théorème des nombres premiers (sans preuve), algorithme d'Euclide, théorème de Gauss, théorème de Bézout, théorème chinois, calcul de la fonction d'Euler, petit théorème de Fermat, équations diophantiennes, résultant.

**TP :** Algorithmes d'Euclide, cribles des nombres premiers. Chiffrement RSA.

---

## Compétences visées

Manipuler des structures algébriques abstraites.

Maîtriser les outils de l'arithmétique nécessaires à la résolution d'équations diophantiennes classiques.

## Infos pratiques

---

### Lieux

› Le Bourget-du-Lac (73)

---

### Campus

› Le Bourget-du-Lac / campus Savoie Technolac