Structures quotients & arithmétique des polynômes et des nombres entiers

ECTS crédits

Composante Sciences et Montagne

En bref

- **Langues d'enseignement:** Français
- **Méthode d'enseignement:** En présence
- **Ouvert aux étudiants en échange:** Non

Présentation

Description

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

Objectifs

Manipuler des structures algébriques abstraites.

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

Heures d'enseignement

Structures quotients & arithmétique des polynômes et des nombres entiers - CM	Cours Magistral	24h
Structures quotients & arithmétique des polynômes et des nombres entiers - TD	Travaux Dirigés	24h
Structures quotients & arithmétique des polynômes et des nombres entiers - TP	Travaux Pratiques	6h

Pré-requis nécessaires

Enseignements d'algèbre de première année.

Plan du cours

- Compléments de MATH201 - 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 **Z**/n**Z**, groupe symétrique Sn (générateurs et groupes alternés An) et sous-groupes de (**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 **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.

Infos pratiques

Lieux

› Le Bourget-du-Lac (73)

Campus

› Le Bourget-du-Lac / campus Savoie Technolac