Groupes et arithmétique

GA4 (6 ECTS, coef. 2)

Type d'UE : fondamentale *(soumise à une note plancher de 8/20 pour être validée)*
Modalités d'évaluation : contrôle continu et examen terminal
Pré-requis : S1, S2, S3 Mathématiques
Parcours intégrant obligatoirement cette UE :
Parcours pouvant intégrer cette UE : Mathématiques, et tout autre parcours, à l'appréciation du directeur des études.

Programme des enseignements

Relation d'équivalence
- définition, classes d'équivalence, partition d'un ensemble ; exemples ;
- ensemble quotient, projection canonique, passage au quotient d'une application.

Arithmétique dans $\mathbb{Z}$
- multiples et diviseurs, division euclidienne, pgcd, ppcm ; relation de Bézout ; théorème de Gauss ; résolution de l'équation $ax+by = c$ dans $\mathbb{Z}$;
- congruences.

Groupes
- groupe, sous-groupe, morphisme et isomorphisme de groupes ; groupe produit ; groupe engendré par un élément ;
- ordre d'un élément ; groupe cyclique ;
- classes modulo un sous-groupe, théorème de Lagrange ; sous-groupe distingué, groupe quotient et passage au quotient d'un morphisme ;
- goupe $\mathbb{Z}/n\mathbb{Z}$ et étude des groupes cycliques ;
- classes de conjugaison.

Anneaux et corps commutatifs
- anneau commutatif unitaire, sous-anneau, morphisme et isomorphisme d'anneaux ; anneau produit ; groupe des inversibles ; anneau quotient $A/(a)$ et passage au quotient d'un morphisme ;
- anneau $\mathbb{Z}/n\mathbb{Z}$; isomorphisme du théorème chinois ; la fonction d'Euler ;
- caractéristique d'un corps ; corps $\mathbb{F}_p$; le groupe des carrés dans $(\mathbb{F}_p)^*$;
- Si $\mathbb{K}$ est un corps fini, alors le groupe $\mathbb{K}^*$ est cyclique ; application à des critères de primalité.

Construction de corps
- polynômes irréductibles ; irréductibles de $\mathbb{R}[X]$, de $\mathbb{C}[X]$, exemples de polynomes irréductibles sur $\mathbb{F}_p$;
- corps $L = \mathbb{K}[X]/(P)$, où K est un corps (commutatif) et $P \in \mathbb{K}[X]$ est irréductible ; dimension de l'espace vectoriel L sur K ;
- exemples de corps finis et de corps de nombres.

Objectifs : Approfondir la notion de groupe. En donner des exemples classiques et des applications en arithmétique. Ces notions, fondamentales en mathématiques, apparaissent dans divers concours de recrutement et sont couramment utilisées en Informatique (cryptologie) et en Chimie (cristallographie) par exemple.