3MA262 – Structures algébriques. Applications.
L3-S2 (6 ECTS, 12 semaines)

Professeur : Pierre-Vincent Koseleff
mél : pierre-vincent.koseleff@upmc.fr,
url : https://webusers.imj-prg.fr/~pierre-vincent.koseleff/

Objectifs de l'UE : Ce cours est une introduction aux structures de base en algèbre, avec en plus, un point de vue effectif. Ce cours est destiné à tous les étudiants de Licence qui souhaitent compléter leur formation en algèbre de base avant de poursuivre en Master de Mathématiques ou en Informatique/Mathématiques.

Prérequis : Connaissances générales en algèbre de niveau L2.

Thèmes abordés :

1. **Structures algébriques de base**
   Groupes, anneaux, corps, espaces vectoriels, algèbres. Anneau factoriel, principal, euclidien. Anneaux de polynômes.
2. **Structures quotient**
   Structure quotient. Théorèmes d'isomorphisme. *Exemples*. Théorème Chinois. *Interpolation de Lagrange.* Caractères des groupes abéliens finis. *Théorème de structure*.
3. **Algorithme d'Euclide**
   Calculs du pgcd, des coefficients de Bézout. Aspects effectifs. Cas de $\mathbf{Z}$ et $K[X]$. *Applications aux calculs dans les structures quotient.* Calcul modulaire. *Protocole cryptographique RSA*.
4. **Extensions algébriques.**
   Éléments algébriques et transcendants. Application à la théorie algébrique des nombres.
5. **Corps finis**
   Existence et construction des corps finis. Isomorphismes. *Algorithme de Berlekamp*
6. **Transformée de Fourier discrète**
   Groupe dual de $\mathbf{Z}/n\mathbf{Z}$. Isomorphismes entre $K[\mathbf{Z}/n\mathbf{Z}] \simeq K[X]/(X^n-1) \simeq K[\widehat{\mathbf{Z}/n\mathbf{Z}}]$. *Transformée de Fourier rapide, applications.*

Équipe pédagogique

Benjamin Girard, Pierre-Vincent Koseleff, Benoît Stroh, Leonardo Zapponi