

MASTER MATHÉMATIQUES ET APPLICATIONS

**PARCOURS MATHÉMATIQUES FONDAMENTALES**

**Semestre 7**

**Option (1 au choix)**

# Algèbre orienté informatique

## Présentation

### Codage:

- > Rappels sur les corps finis: construction de corps finis, algèbre linéaire sur un corps fini, anneau de polynômes en une indéterminée sur un corps fini, cyclicité du groupe multiplicatif
- > Codes correcteurs d'erreurs linéaires. Longueur, dimension, distance, capacité de correction d'un code. Borne de Singleton. Matrice génératrice d'un code, matrice de parité d'un code
- > Exemples de codes: codes polynomiaux, codes cycliques, codes de Hamming, codes BCH, codes de Reed-Solomon (codage et décodage, correction d'erreurs)

### Cryptographie:

- > Systèmes de chiffrement simples: chiffrements affine et linéaire
- > Le chiffrement RSA
- > L'échange de clé publique Diffie-Hellman
- > Le chiffrement Massey-Omura
- > Le chiffrement ElGamal
- > Fonctions de hachage et la signature DSS
- > Le problème du logarithme discret

### Modélisation géométrique:

- > Courbes et surfaces paramétrées, courbes et surfaces polynomiales et rationnelles.
- > Polynômes de Bernstein et courbes et surfaces de Bézier. Polarisation d'un polynôme et l'algorithme de De Casteljau. La méthode de sous-division pour approcher les courbes et surfaces polynomiales.

Implicitisation des courbes et surfaces rationnelles. Idéal d'élimination. Résultants, théorèmes de projection et d'élimination et d'implicitisation. Bases de Groebner.

## Bibliographie

Lindsay Childs: A concrete introduction to higher algebra.  
 Lekh Vermani: Elements of algebraic coding theory.  
 Neil Koblitz: A course in number theory and cryptography.  
 Jean Gallier: Curves and surfaces in geometric modeling. Theory and algorithms.  
 Cox, Little O'Shea : Ideals, varieties and algorithms.

## Modalités de contrôle des connaissances

### Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CC	Ecrit et/ou Oral		1/1	NF= $\max(\min((N1+N2)/2, 10), (N1+N2+N3)/3, N3)$ - Pas de session 2 -

### Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
	Autre modalité	Autre nature			Pas de session 2

# Méthodes numériques

## Présentation

1- Résolution de systèmes linéaires et non linéaires :  
Méthodes des directions alternées, stationnaires et instationnaires, méthodes de Krylov, techniques de préconditionnement, méthodes de Newton-Kantorovich (version exacte et variante inexacte).  
2- Calcul spectral :  
Méthodes de la puissance, puissance inverse, quotient de Rayleigh et de Lanczos incomplète.  
3- Programmation et application des méthodes étudiées sur des problèmes concrets.

### 5 crédits ECTS

Volume horaire

Travaux Dirigés : 22h

Cours Magistral : 22h

## Bibliographie

L.Amodei, J.-P. Dedieu, Analyse numérique matricielle, Dunod, 2008. A. Quarteroni, F. Saleri, P. Gervasio, Scientific computing with MATLAB and Octave, Springer, 2014

## Modalités de contrôle des connaissances

### Session 1 ou session unique - Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
UE	CC	Ecrit et/ou Oral		1/1	NF=max(min((N1+N2)/2,10), (N1+N2+N3)/3,N3) - Pas de session 2 -

### Session 2 : Contrôle de connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Coefficient	Remarques
	Autre modalité	Autre nature			Pas de session 2