

# Savoir-faire et thèmes classiques – Structures algébriques et arithmétique

## 1 Structures algébriques

### Savoir-faire

- Utiliser la définition d'un groupe, d'un groupe abélien
- Connaître les groupes classiques
- Utiliser la caractérisation d'un sous-groupe, reconnaître un groupe en tant que produit cartésien, qu'intersection, que groupe engendré par une partie, image directe ou réciproque d'un sous-groupe par un morphisme de groupe (par exemple son noyau ou son image), ensemble des inversibles d'un anneau
- Connaître les sous-groupes de  $(\mathbb{Z}, +)$
- Montrer qu'on a un morphisme de groupe, calculer son noyau
- Traduire l'injectivité et la surjectivité d'un morphisme de groupe avec son noyau ou son image
- Définir le sous-groupe engendré par une partie, décrire ses éléments
- Utiliser la définition d'un anneau, d'un anneau commutatif
- Connaître les anneaux classiques
- Faire des calculs dans un anneau avec hypothèses adaptées (binôme,  $a^n - b^n$ , somme géométrique...)
- Utiliser la définition d'un corps
- Connaître les corps classiques
- Utiliser la définition d'un anneau intègre, la régularité de ses éléments, le fait qu'un corps le soit
- Reconnaître un sous-anneau, un anneau comme anneau produit, un sous-corps

- Montrer qu'on a un morphisme d'anneaux, calculer son noyau
- Définir un idéal d'un anneau commutatif
- Voir le noyau d'un morphisme d'anneau comme un idéal, l'image comme un sous-anneau
- Définir un idéal et un anneau principal
- Caractériser la divisibilité avec les idéaux, définir les PGCD et PPCM en termes d'idéaux
- Utiliser la définition d'une algèbre
- Connaître les algèbres classiques
- Définir un polynôme en un élément d'une algèbre
- Définir un morphisme d'algèbres

### Thèmes Classiques

- CNS pour qu'une réunion de sous-groupes (ou sev) le soit encore
- (\*) Sous-groupes de  $(\mathbb{R}, +)$
- Théorème de Lagrange
- Centre d'un groupe
- (\*) Sous-groupes distingués
- Idéaux annulateurs, premiers
- Nilpotents d'un anneau
- Entiers de Gauß
- Anneau de Boole  $(\mathcal{P}(E), \Delta, \cap)$
- (\*) Radical d'un idéal



## 2 Arithmétique entière

### Savoir-faire

- Définir PGCD et PPCM à l'aide d'idéaux, les caractériser à l'aide de l'ordre partiel de division, les calculer à partir de décompositions primaires
- Utiliser la propriété d'Euclide, l'algorithme d'Euclide, l'algorithme d'Euclide étendu
- Résoudre une équation diophantienne  $ax + by = c$  dans  $\mathbb{Z}$
- Définir des nombres premiers entre eux, s'y ramener par factorisation du PGCD, utiliser le théorème de Bézout, le lemme de Gauß, et les autres propriétés du programme les concernant
- Définir les nombres premiers, utiliser leurs propriétés, montrer qu'ils sont en nombre infini, écrire une décomposition primaire
- Définir une valuation  $p$ -adique et connaître ses propriétés
- Définir la relation de congruence modulo  $n$ , traduire que deux nombres sont congrus modulo  $n$  par un argument de divisibilité
- Connaître les critères de divisibilité par 2, 3, 4, 5, 8, 9, 10, 11
- Obtenir une divisibilité par calcul modulaire
- Connaître le petit théorème de Fermat
- Calculer les puissances d'un entier modulo  $n$  : soit en trouver une cyclicité à la main, soit en utilisant le petit théorème de Fermat

### Thèmes Classiques

- Nombres de Mersenne et de Fermat
- Formule de Legendre
- Triplets pythagoriciens
- Fonction et inversion de Möbius
- Chiffrement RSA