

MPSI 2  
Programme des colles de mathématiques.  
Semaine 12 : du lundi 8 janvier au vendredi 12.

**Liste des questions de cours**

- 1°) Si  $B$  est une partie d'un anneau commutatif, quels sont les éléments de l'idéal engendré par  $B$ ? Démontrez-le.
- 2°) Montrer que  $\mathbb{Z}$  est un anneau principal.
- 3°) Que peut-on dire de l'image réciproque d'un idéal par un morphisme d'anneaux? Démontrez-le.
- 4°) Si  $H$  est un sous-groupe d'un groupe commutatif  $(G, +)$ , définir  $G/H$  et montrer qu'on peut le munir naturellement d'une loi de groupe abélien.
- 5°) Montrer que tout groupe cyclique d'ordre  $n$  est isomorphe à  $\mathbb{Z}/n\mathbb{Z}$ .
- 6°) Quels sont les sous-groupes (resp : les idéaux) de  $\mathbb{Z}/n\mathbb{Z}$ ?
- 7°) Déterminer l'ensemble des générateurs du groupe  $(\mathbb{Z}/n\mathbb{Z}, +)$  et l'ensemble des éléments inversibles de l'anneau  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ .
- 8°) Énoncer et démontrer le théorème chinois.
- 9°) Pour  $h_1, \dots, h_n \in \mathbb{Z}$ , méthode de calcul de  $\ell \in \mathbb{Z}$  tel que, pour tout  $i \in \{1, \dots, n\}$ ,  $\ell \equiv h_i$  modulo  $a_i$ , où  $a_1, \dots, a_n$  sont deux à deux premiers entre eux,
- 10°) Si  $a \wedge b = 1$ , montrer que l'indicatrice d'Euler vérifie  $\varphi(ab) = \varphi(a)\varphi(b)$ .
- 11°) Pour tout  $n \in \mathbb{N}^*$ , montrer que  $n = \sum_{d \in \mathbb{N}, d|n} \varphi(d)$ .

**Thèmes de la semaine : groupes, anneaux et corps.**

**1 Les groupes : En révisions**

Le programme de colles précédent est à réviser et peut faire l'objet d'exercices.

**2 La structure d'anneau**

Définition d'un anneau, règles usuelles de calcul dans un anneau.

Si  $A$  n'est pas l'anneau nul, alors  $1_A \neq 0_A$ .

Sous-anneaux.

Groupe des inversibles. Définition d'un corps (toujours commutatif). Sous-corps.

Formule du binôme de Newton et du multinôme, formule de Bernoulli.

Diviseurs de 0, anneaux intègres.

Morphismes d'anneaux. Composée, isomorphisme réciproque, image directe ou réciproque d'un sous-anneau.

Un morphisme de corps est toujours injectif.

Anneau produit.

### 3 Les idéaux

Idéal à gauche ou à droite d'un anneau. Les idéaux sont des sous-groupes.

Si  $I$  est un idéal,  $1 \in I \iff I = A$ .

Intersection d'idéaux, idéal engendré par une partie  $B$ , noté  $Id(B)$ .

**Notation.** Pour la suite, on fixe un anneau  $(A, +, \cdot)$  que l'on suppose commutatif.

$$Id(B) = \left\{ \sum_{i=1}^n a_i b_i / n \in \mathbb{N}, (a_1, \dots, a_n) \in A^n, (b_1, \dots, b_n) \in B^n \right\}.$$

Idéal principal, anneau principal.

$\mathbb{Z}$  est un anneau principal.

Somme de deux idéaux, image réciproque d'un idéal par un morphisme d'anneaux.

### 4 Groupes et anneaux quotients

Si  $(G, +)$  est commutatif, définition du groupe quotient  $G/H$ . Surjection canonique de  $G$  dans  $G/H$ .

Cas particulier fondamental :  $\mathbb{Z}/n\mathbb{Z}$ .

Tout groupe cyclique est isomorphe à un  $\mathbb{Z}/n\mathbb{Z}$ .

Définition de l'anneau quotient  $A/I$ , lorsque  $I$  est un idéal de l'anneau commutatif  $A$ .

Règles de calcul dans l'anneau  $\mathbb{Z}/n\mathbb{Z}$ .

### 5 $\mathbb{Z}/n\mathbb{Z}$

Générateurs du groupe  $(\mathbb{Z}/n\mathbb{Z}, +)$ , éléments inversibles de l'anneau  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ .

$\mathbb{Z}/n\mathbb{Z}$  est un corps (resp : est intègre) si et seulement si  $n \in \mathbb{P}$ .

**Théorème chinois :** Si  $a_1, \dots, a_n$  sont deux à deux premiers entre eux,  

$$\begin{array}{ccc} \mathbb{Z}/(a_1 \times \dots \times a_n)\mathbb{Z} & \longrightarrow & (\mathbb{Z}/a_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/a_n\mathbb{Z}) \\ \bar{k} & \longmapsto & (\bar{k}, \dots, \bar{k}) \end{array}$$
 est un isomorphisme d'anneaux.

Pour  $h_1, \dots, h_n \in \mathbb{Z}$ , méthode de calcul de  $\ell \in \mathbb{Z}$  tel que, pour tout  $i \in \{1, \dots, n\}$ ,  $\ell \equiv h_i$  modulo  $a_i$ .

**Indicatrice d'Euler :** Pour tout  $n \in \mathbb{N}^*$ , on pose  $\varphi(n) = |U(\mathbb{Z}/n\mathbb{Z})|$ .

Si  $p$  est premier et si  $k \in \mathbb{N}^*$ ,  $\varphi(p^k) = p^k - p^{k-1}$ .

Si  $a \wedge b = 1$ , alors  $\varphi(ab) = \varphi(a)\varphi(b)$ .

Pour tout  $n \in \mathbb{N}^*$ ,  $n = \sum_{d \in \mathbb{N}, d|n} \varphi(d)$ .

Euler-Fermat : si  $k \wedge n = 1$ , alors  $k^{\varphi(n)} \equiv 1$  modulo  $n$ .

Petit théorème de Fermat : Si  $p$  est un nombre premier,  $\forall k \in \mathbb{Z}$ ,  $k^p \equiv k$  modulo  $p$ .

## 6 Caractéristique d'un anneau commutatif

$\text{car}(A) = n \iff \text{Ker}(\varphi) = n\mathbb{Z}$ , où  $\varphi : \mathbb{Z} \longrightarrow A$   
 $m \longmapsto m \cdot 1_A$ .

Deux anneaux isomorphes ont la même caractéristique.

Le plus petit sous-anneau de  $A$  est isomorphe à  $\mathbb{Z}/n\mathbb{Z}$ , où  $n = \text{car}(A)$ .

Un anneau de caractéristique nulle est de cardinal infini.

Si  $A$  est intègre et  $\text{car}(A) \neq 0$ , alors  $\text{car}(A) \in \mathbb{P}$ .

Endomorphisme de Frobenius, sur un anneau de caractéristique  $p \in \mathbb{P}$ .

La caractéristique d'un corps est ou bien nulle, ou bien un nombre premier.

Description du sous-corps premier de  $\mathbb{K}$ .

### Prévisions pour la semaine prochaine :

Espaces vectoriels, théorie de la dimension.