Semaine du 22/11 au 26/11

1 Cours

Révisions de première année : arithmétique de $\mathbb{Z}$ et $\mathbb{K}[X]$

Anneaux, arithmétique

Anneaux Définition d'un anneau. Groupe des inversibles. Règle de calculs : $\forall a \in A,\ 0_A \times a = a \times 0_A = 0_A$; $\forall (a,b,n) \in A^2 \times \mathbb{Z},\ n(a \times b) = (na) \times b = a \times (nb)$. Intégrité. Anneau produit. Sous-anneau. Morphisme d'anneaux. L'image d'un morphisme d'anneau est un sous anneau.

Corps Définition. Un corps est intègre. Sous-corps. Morphismes de corps.

Idéaux Définition. Idéal engendré par une partie. Le noyau d'un morphisme d'anneaux est un idéal. Divisibilité dans un anneau et interprétation en termes d'idéaux principaux : $a \mid b \iff bA \subset aA$.

Aritmétique de $\mathbb{Z}$ Rappels. Idéaux de $\mathbb{Z}$. Interprétation du PGCD et du PPCM en termes d'idéaux : $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$; $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

Aritmétique de $\mathbb{K}[X]$ Rappels. Idéaux de $\mathbb{K}[X]$. Interprétation du PGCD et du PPCM en termes d'idéaux : $P\mathbb{K}[X]+Q\mathbb{K}[X] = (P \wedge Q)\mathbb{K}[X]$; $P\mathbb{K}[X] \cap Q\mathbb{K}[X] = (P \vee Q)\mathbb{K}[X]$.

Anneau $\mathbb{Z}/n\mathbb{Z}$ Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$. Inversibles de $\mathbb{Z}/n\mathbb{Z}$: $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si $k \wedge n = 1$. $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier. Théorème des restes chinois : si $m \wedge n = 1$, l'application $\begin{cases} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{k}^{mn} & \longmapsto & \left(\overline{k}^{m}, \overline{k}^{n}\right) \end{cases}$ est bien définie et est un isomorphisme d'anneaux. Indicatrice d'Euler. Expression à l'aide de la décomposition en facteurs premiers : si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, alors $\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$. Théorème d'Euler : si $a \wedge n = 1$, $a^{\varphi(n)} \equiv 1[n]$.

Algèbre Structure d'algèbre. Sous-algèbre. Morphisme d'algèbres.

2 Méthodes à maîtriser

- Montrer qu'un ensemble est un anneau/un corps/une algèbre en montrant que c'est un sous-anneau/un sous-corps/une sous-algèbre de d'un anneau/d'un corps/d'une algèbre connu.
- Attention aux calculs dans un anneau : a priori, un anneau n'est ni commutatif ni intègre (exemples : $\mathcal{M}_n(\mathbb{K})$, $\mathcal{L}(E)$).
- Techniques classiques d'arithmétique dans $\mathbb{Z}$:
  - utilisation du lemme de Gauss ou du lemme d'Euclide ;
  - règles de calcul avec les congruences ;
  - montrer que deux entiers sont premiers entre eux : montrer que leur seul diviseur commun est 1 / exhiber relation de Bézout / montrer qu'ils n'admettent pas de diviseur premier commun ;
  - montrer qu'un entier naturel est premier : il est différent de 1 et ses seuls diviseurs sont 1 et lui-même ;
  - montrer que deux entiers sont égaux en montrant qu'ils se divisent l'un l'autre.
- Factorisation d'un polynôme en un produit de facteurs irréductibles :
  - déterminer les racines ;
  - caractériser la multiplicité d'une racine via les dérivées successives ;
  - si P est pair/impair, a est racine de P de multiplicité m si et seulement si $-a$ est racine de P de multiplicité m ;
  - si P est à coefficients **réels**, $a \in \mathbb{C}$ est racine de P de multiplicité m si et seulement si $\overline{a}$ est racine de P de multiplicité m.
- Résoudre un système de congruences du type $\begin{cases} x \equiv a[m] \\ x \equiv b[n] \end{cases}$.
- Résoudre une équation diophantienne linéaire du type $ax + by = c$.
- Ne pas s'emmêler les pinceaux entre les différentes structures :
  - $(\mathbb{Z}, n\mathbb{Z}, +)$ est un **groupe** ;
  - $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un **anneau** et un **corps** si n est **premier** ;
  - $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ (ensemble des **inversibles** de $\mathbb{Z}/n\mathbb{Z}$) est un **groupe**.

3 Questions de cours

Banque CCP Exos 66, 85, 86, 87, 90, 94.