Chapitre 3

Anneaux, corps, algèbres, idéaux

1. Anneaux, corps, algèbres

1.1. Anneau

a) Définition

b) Exemple

c) Groupe des inversibles d'un anneau

d) Produit d'anneaux

e) Relation de divisibilité dans un anneau A.

f) Sous-anneau : définition, caractérisation

g) Morphisme d'anneaux

1.2. Anneau intègre

1.3. Corps

a) Définition

b) Sous-corps : définition, caractérisation

1.4. Algèbre

a) Définition, exemples

b) Sous-algèbre : définition, caractérisation

2. L'anneau $\mathbb{Z}/n\mathbb{Z}$

2.1. Rappels sur les congruences

2.2. Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$

2.3. Théorème chinois

Théorème chinois : Isomorphisme entre $\mathbb{Z}/(mn)\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Corollaire en terme de congruences : démonstration à l'aide du théorème

2.4. Eléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$

a) Le théorème fondamental : démonstration

b) Cas où $p \in \mathbb{P}$: théorème CNS pour que $\mathbb{Z}/p\mathbb{Z}$ soit un corps démonstration

c) Fonction indicatrice d'Euler :

- Définition et interprétation
- Propriété 1 : $\forall (m,n) \in \mathbb{N}^{*2}$: $[m \wedge n = 1] \Rightarrow \varphi() = \varphi(m) \times \varphi(n)$

- Propriété 2 : $\forall p \in \mathbb{P},\ \forall \alpha \in \mathbb{N} : \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$
- Expression de $\varphi\ n$ démonstration

d) Théorème d'Euler : démonstration

e) Petit théorème de Fermat : démonstration

3. Idéaux

3.1. Définition et exemple

3.2. Propriété : le noyau d'un morphisme d'anneaux est un idéal démonstration

3.3. Divisibilité et idéaux

3.4. Intersection et somme d'idéaux démonstration

3.5. Conséquence 1 : arithmétique dans $\mathbb{Z}$

a) Idéaux de $\mathbb{Z}$

b) Définition du PPCM par $\boxed{a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}}$

c) Définition du PGCD par $\boxed{a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}}$

d) Conséquence : théorème de Bezout, théorème de Gauss (réviser)

e) Savoir faire : un (au moins) algorithme de recherche des coefficients de Bezout

3.6. Conséquence 2 : arithmétique dans $K[X]$

a) Idéaux de $K[X]$: démonstration

b) Définition du P.G.C.D. de deux polynômes par $(A) + (B) = (D)$

c) Conséquence : théorème de Bezout, théorème de Gauss (réviser)

d) Polynômes irréductibles de $K[X]$

- Définition, caractérisation de la non irréductibilité : polynôme scindé
- Théorème de décomposition en polynômes irréductibles (rappel)
- Polynômes irréductibles de $\mathbb{C}\ X$, théorème de D'Alembert (rappel)
- Polynômes irréductibles de $\mathbb{R}\ X$ (rappel)