Développements :

- Théorème chinois
- L'anneau des entiers de Gauss

Références :

- Algèbre - Le grand combat, Berhuy
- Algèbre linéaire, Grifone
- Anneaux, corps, résultants, Ulmer
- Cours d'algèbre, Perrin

On fixe un anneau commutatif unitaire **intègre** A.

1. Anneaux principaux

1.1. Idéaux [Berhuy]

- Def : idéal principal
- Def : anneau principal
- Ex : $\mathbb{Z}$, $K[X]$ si K est un corps
- Contre-ex : $\mathbb{Z}[X]$ (l'idéal $(2, X)$ n'est pas principal)
- Def : idéal premier
- Ex : si p est un nombre premier, alors $p\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$
- Def : idéal maximal
- Thm : si I est un idéal de A, alors
  - I est premier ssi A/I est intègre
  - I est maximal ssi A/I est un corps
    En particulier, si I est maximal alors I est premier.

1.2. Arithmétique des anneaux principaux [Berhuy]

- Def : divisibilité
- Def : éléments premiers entre eux
- Ex : X et Y sont premiers entre eux dans $\mathbb{Z}[X, Y]$
- Def : pgcd, ppcm
- Def : élément irréductible
- Ex :
  - les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1

    - les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1, et ceux de degré 2 à discriminant < 0
- Def : élément premier
- Ex : tout nombre premier est un élément premier de $\mathbb{Z}$
- Prop : si A est principal, $(a) + (b) = (d)$ et $(a) \cap (b) = (m)$, alors :
    - d est un pgcd de a et b
    - m est un ppcm de a et b
- Cor : si A est principal, alors $a, b \in A$ sont premiers entre eux ssi il existe $u, v \in A$ tels que $au + bv = 1$
- Lemme (Gauss) : si A est principal et $a, b \in A$ sont premiers entre eux, alors pour tout $c \in A$, $a \mid bc$ entraîne $a \mid c$
- Lemme (Euclide) : si A est principal et $\pi \in A$ est irréductible, alors pour tous $a, b \in A$, $\pi \mid ab$ entraîne $\pi \mid a$ ou $\pi \mid b$
- Cor : si A est principal, alors tout idéal premier non nul de A est maximal

1.3. Factorialité des anneaux principaux [Perrin]

- Def : anneau factoriel avec (E) et (U)
- Prop : si A vérifie (E), s'équivalent :
    - A vérifie (U)
    - A vérifie le lemme d'Euclide
    - tout élément irréductible de A est premier
    - A vérifie le lemme de Gauss
- Prop : si A est principal, alors tout élément irréductible de A est premier
- Cor : si A est principal, alors A est factoriel

1.4. Théorème chinois [Ulmer]

- Thm : si $I_1, \dots, I_n$ sont des idéaux de A deux à deux comaximaux, alors l'application $\varphi : A \to A/I_1 \times \cdots \times A/I_n$ définie par $\varphi(a) = (a \bmod I_1, \dots, a \bmod I_n)$ est un morphisme surjectif de noyau $I_1 \cdots I_n = \bigcap_{k=1}^{n} I_k$, induisant un isomorphisme d'anneaux $A/(I_1 \cdots I_n) \cong A/I_1 \times \cdots \times A/I_n$
- Cor : pour tous $\beta_1, \dots, \beta_n \in A$, le système de congruences $\{x \equiv \beta_k \bmod I_k\}$ admet une unique solution modulo $I_1 \cdots I_n$
- Cor : si A est principal et $m_1, \dots, m_n \in A$ sont premiers entre eux 2 à 2, alors $A/m_1 \cdots m_n \cong A/m_1 \times \cdots \times A/m_n$ (en particulier, le système ci-dessus admet pour tous $\beta_1, \dots, \beta_n \in A$ une unique solution dans $A/m_1 \cdots m_n$)
- Cor : si K est un corps, $\alpha_0, \dots, \alpha_n \in K$ sont deux à deux distincts et $\beta_0, \dots, \beta_n \in K$, il existe un unique $g \in K[X]$ de degré $\leq n$ tel que $g(\alpha_i) = \beta_i$ pour tout $i \in \{0, \dots, n\}$

- Rmq : le problème d'interpolation correspond au calcul d'un antécédent g de $(\beta_0, \dots, \beta_n)$ de degré $\leq n$, pour le morphisme $K[X] \to K^{n+1}$ défini par $f \longmapsto (f(\alpha_0), \dots, f(\alpha_n))$

2. Anneaux euclidiens et calculs effectifs

2.1. Résultats théoriques généraux [Perrin]

- Def : anneau euclidien
- Ex : $\mathbb{Z}$, $K[X]$ si K est un corps, $\mathbb{Z}[i]$, $\mathbb{Z}[j]$
- Prop : si A est euclidien, alors A est principal
- Contre-ex : $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ est principal mais non euclidien
- Rmq : contrairement au cas principal, on dispose ici d'algorithmes

2.2. L'anneau des entiers de Gauss [Perrin]

- Def : $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$
- Prop : $\mathbb{Z}[i]^\times = \{-1, 1\}$
- Prop : $\mathbb{Z}[i]$ est un anneau euclidien
- Thm : si p est un nombre premier impair, s'équivalent :
  - p est somme de deux carrés
  - $p \equiv 1 \bmod 4$
- Thm : si $n \in \mathbb{N}_{\geq 2}$, s'équivalent :
  - n est somme de deux carrés
  - pour tout nombre premier $p \equiv 3 \bmod 4$, $v_p(n)$ est pair
- Thm : les irréductibles de $\mathbb{Z}[i]$ sont, aux inversibles près :
  - les nombres premiers $p \equiv 3 \bmod 4$
  - les éléments dont la norme est un nombre premier

2.3. Calculs de PGCD [Berhuy, Ulmer]

On se place dans un anneau euclidien A.

- Principe de l'algorithme d'Euclide
- Principe de l'algorithme d'Euclide généralisé
- Ex : détermination d'une relation de Bézout entre deux entiers
- App : calcul d'inverses dans les anneaux quotients et notamment les corps finis, par exemple l'inverse de $X^2 + X + 1$ dans $\mathbb{F}_2[X]/(X^3 + X^2 + 1)$
- Rmq : calcul en $\mathrm{O}(n^2)$ où n est la taille des entrées

2.4. Congruences et interpolation [Ulmer]

- Principe de l'algorithme : si A est euclidien de stathme $\nu : A \setminus \{0\} \to \mathbb{N}$, on peut résoudre le système de congruences $\{x \equiv \beta_k \bmod m_k\}$ par décomposition en "base mixte", c'est-à-dire calculer une solution x de la forme $x = \gamma_1 + \gamma_2 m_1 + \gamma_3 (m_1 m_2) + \cdots + \gamma_n (m_1 \dots m_{n-1})$ avec $\nu(\gamma_i) < \nu(m_i)$, en calculant dans l'ordre les coefficients indéterminés γ_i
- Ex : résolution du système $x \equiv 1 \bmod 3$, $x \equiv 3 \bmod 5$, $x \equiv 0 \bmod 7$ dans $\mathbb{Z}$
- Ex : recherche de $f \in \mathbb{F}_5[X]$ tel que $f(0) = 2$, $f(1) = 0$ et $f(2) = 1$

3. Applications en algèbre linéaire [Grifone]

- Prop : si E est un K-e.v. de dimension finie et $u \in \mathscr{L}(E)$, alors l'idéal $\{P \in K[X] \mid P(u) = 0\}$ est principal
- Def : polynôme minimal π_u (ou π_A pour une matrice A)
- Prop : u est diagonalisable ssi π_u est scindé à racines simples ssi u admet un polynôme annulateur scindé à racines simples
- Ex : $A = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$ est diagonalisable car $\pi_A = (X+2)(X-1)$
- Contre-ex : $B = \begin{pmatrix} 3 & -1 & 1 \\ 2 & 0 & 1 \\ 1 & -1 & 2 \end{pmatrix}$ n'est pas diagonalisable car $\pi_B = (X-1)(X-2)^2$