Développements :

- Théorème chinois
- Suites de Sturm

Références :

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

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

1. Cadre théorique général

1.1. Notions de PGCD et PPCM [Berhuy, Rombaldi]

- Def : divisibilité
- Def : éléments premiers entre eux
- Ex : X et Y sont premiers entre eux dans $\mathbb{Z}[X,Y]$
- Def : pgcd, ppcm
- Ex : $\mathrm{pgcd}(14,12)=2$ dans $\mathbb{Z}$ (ici on a un choix "canonique" de pgcd donné par l'unique positif, idem dans $K[X]$ où K est un corps)
- Thm : si $a_1,\dots,a_r \in A\setminus\{0\}$ et d est un diviseur commun aux a_i avec $a_i = db_i$, alors $d \sim \mathrm{pgcd}(a_1,\dots,a_r)$ ssi $\mathrm{pgcd}(b_1,\dots,b_r)\sim 1$
- Lemme (Gauss) : si $a,b\in A$ sont premiers entre eux, alors pour tout $c\in A$, $a \mid bc$ entraîne $a\mid c$

1.2. Anneaux factoriels [Perrin]

1.2.1. Résultats généraux

- Def : A factoriel
- Ex : $\mathbb{Z}$, $K[X]$ si K est un corps, $\mathbb{Z}[X]$
- Def : valuation p-adique pour p irréductible
- Prop : si $a,b\in A$, alors a et b ont un pgcd et un ppcm, et si $a\sim\prod p^{v_p(a)}$ et $b\sim\prod p^{v_p(b)}$:
  - $\mathrm{pgcd}(a,b)\sim\prod p^{\min(v_p(a),v_p(b))}$
  - $\mathrm{ppcm}(a,b)\sim\prod p^{\max(v_p(a),v_p(b))}$

1.2.2. Polynômes à coefficients dans un anneau factoriel

- Def : contenu $c(P)$ de $P \in A[X]$ pour A factoriel
- Def : $P \in A[X]$ est dit primitif lorsque $c(P) = 1$
- Lemme (Gauss) : si A est factoriel et $P, Q \in A[X]$, alors $c(PQ) \sim c(P)c(Q)$
- Thm : si A est factoriel, les irréductibles de $A[X]$ sont :
  - les constantes irréductibles de A
  - les polynômes primitifs de $A[X]$ de degré ≥ 1, irréductibles sur $\mathrm{Frac}(A)$
- Thm (Gauss) : si A est factoriel, alors $A[X]$ est factoriel

1.3. Anneaux principaux [Berhuy, Rombaldi]

- 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)
- 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
- Rmq : ça ne permet pas de calculer ces éléments, il faut des algorithmes
- Thm : si A est principal, alors A est factoriel
- Thm (Bézout) : si A est principal, alors $a, b \in A$ sont premiers entre eux ssi il existe $u, v \in A$ tels que $au + bv = 1$
- Cor : si A est principal, $a, b, c \in A \setminus \{0\}$ et c est premier avec a, alors $\mathrm{pgcd}(a, bc) = \mathrm{pgcd}(a, b)$
- Cor : si A est principal, $a_1, \dots, a_r \in A \setminus \{0\}$ et c est premier avec chaque a_i, alors c est premier avec $a_1 \cdots a_r$

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. Algorithmes dans les anneaux euclidiens

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. Calculs de PGCD [Rombaldi, 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

2.3. 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 $x=\gamma_1+\gamma_2 m_1+\gamma_3(m_1m_2)+\cdots+\gamma_n(m_1\dots m_{n-1})$ 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 de l'algorithme d'Euclide

3.1. Suites de Sturm [Ulmer]

- Def : pour $f\in\mathbb{R}[X]$ et $a<b$ non racines de f, une suite de Sturm pour f sur $[a,b]$ est une suite $(f_0,\dots,f_r)$ de polynômes de $\mathbb{R}[X]$ tels que :
  - $f_0=f$
  - f_r est sans racine dans $[a,b]$
  - si $f(x)=0$, alors f_0f_1 est strictement croissante au voisinage de x
  - pour tout $i\in\{1,\dots,r-1\}$, si $f_i(x)=0$ alors $f_{i-1}(x)f_{i+1}(x)<0$

- Thm (Sturm) : si $s = (f_0, \dots, f_r)$ est une suite de Sturm pour f sur $[a, b]$, alors le nombre de racines distinctes de f dans $[a, b]$ est $\sigma_s(a) - \sigma_s(b)$, où $\sigma_s(x)$ est le nombre de changements de signes dans la suite $s(x) = (f_0(x), \dots, f_r(x))$
- Thm : si $f \in \mathbb{R}[X]$ sans facteur carré et $a < b$ non racines de f, la suite définie ci-dessous est une suite de Sturm pour f sur $[a, b]$:
  - $f_0 = f$
  - $f_1 = f'$
  - tant que possible, $f_{i-1} = f_i q_i - f_{i+1}$ (division euclidienne de f_{i-1} par f_i)

3.2. Résultants [Ulmer]

- Def : si $f, g \in A[X] \setminus \{0\}$ de degrés respectifs n et m, la matrice de Sylvester de f et g est la matrice de l'application $A_{m-1}[X] \times A_{n-1}[X] \to A_{m+n-1}[X]$ définie par $(u, v) \longmapsto fu + gv$ dans les bases :
  - $((X^{m-1}, 0), \dots, (1, 0), (0, X^{n-1}), \dots, (0, 1))$ de $A_{m-1}[X] \times A_{n-1}[X]$
  - $(X^{m+n-1}, \dots, X, 1)$ de $A_{m+n-1}[X]$
- Def : le résultant $\mathrm{Res}(f, g)$ de f et g est le déterminant de leur matrice de Sylvester
- Prop : $\mathrm{Res}(f, g) = (-1)^{mn} \mathrm{Res}(g, f)$
- Prop : si $f = a_0$ est constant, alors $\mathrm{Res}(f, g) = a_0^m$
- Thm : si $f = gq + r$ (division euclidienne de f par g) avec $r \neq 0$, alors $\mathrm{Res}(f, g) = (-1)^{mn} b_m^{n - \deg(r)} \mathrm{Res}(g, r)$, où b_m est le coefficient dominant de g

Annexe

- Algorithme d'Euclide pour deux entiers
- Un exemple de suite de Sturm