15 Leçon 142 : PGCD et PPCM, algorithmes de calcul. Applications.

I. Notion de PGCD et PPCM

1. Dans un anneau quelconque [ROM]

PGCD, anneau à pgcd, contre-exemple, éléments premiers entre eux, théorème de Gauss, PPCM, commutativité et associativité du pgcd, lien entre pgcd et ppcm

2. Dans un anneau factoriel [ROM]

Anneau factoriel, expression du pgcd, expression du ppcm

3. Dans un anneau principal [ROM] [PER] [ULM]

Anneau principal, exemples, principal $\Rightarrow$ factoriel, expression du pgcd et ppcm avec les idéaux, théorème de Bézout, lemme d'Euclide et de Gauss, contre-exemple au théorème de Bézout dans un anneau factoriel

II. Algorithme de calcul dans un anneau euclidien [ULM] [ROM] [GOU]

Anneau euclidien, exemples, euclidien $\Rightarrow$ principal, algorithme d'Euclide, exemples, algorithme d'Euclide étendu, exemple

III. Applications

1. Théorème chinois [ROM]

DEV 1 : théorème chinois + formule générale de l'indicatrice d'Euler

exemple de système de congruences

2. En algèbre linéaire [MAN] [BER]

Lemme des noyaux, annulateur de u, polynôme minimal, PPCM avec les polynômes minimaux induits

3. Polynômes [PER]

Contenu, DEV 2 : critère d'Eisenstein, exemples

Présentation :

- Le but de cette leçon est de généraliser les notions de PGCD et de PPCM connue dans $\mathbb{Z}$ à d'autres types anneaux afin de pouvoir en tirer de bonnes propriétés arithmétiques.
- Un pgcd ou ppcm n'est pas unique, il est défini à un inversible près.
- Comme tout élément associé à un pgcd de a et b est aussi un pgcd de a et b, et en considérant que 1 est associé à tout élément inversible de A, on peut écrire que a et b sont premiers entre eux ssi $\text{pgcd}(a,b) = 1$.
- Dans un anneau euclidien, on dispose de l'algorithme d'Euclide pour obtenir le pgcd de deux élements, et en remontant cet algorithme on peut trouver une relation de Bézout.
- Dans le lemme des noyaux, c'est le fait que $K[X]$ soit principal et donc qu'il existe une relation de Bézout entre les polynômes qui permet de faire fonctionner la preuve.

Développements :

- Théorème chinois + application à l'indicatrice d'Euler

  - Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi, p249-283

- Critère d'Eisenstein
  - Théorie de Galois, Gozard, p10
  - Cours d'algèbre, Perrin, p51 et 76

Références :

- [ROM] Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi
- [PER] Cours d'algèbre, Perrin
- [ULM] Anneaux-corps-résultants, Ulmer
- [GOU] Algèbre-Probabilités, Gourdon
- [MAN] Algèbre linéaire réduction des endomorphismes, Mansuy-Mneimné
- [BER] Algèbre : le grand combat, Berhuy

Leçon 142 : PGCD et PPCM, algorithmes de calcul. Applications

Soit A un anneau commutatif intègre.

I Notion de PGCD et PPCM

Soit $a_1, \dots, a_n \in A^*$

1) Dans un anneau quelconque [ROM]

ROM 242

Déf 1 : On dit que $a_1, \dots, a_n$ admettent un plus grand commun diviseur s'il existe $\delta \in A^*$ tel que :
$\begin{cases} \forall k \in [\![1; n]\!], \ \delta \text{ divise } a_k \\ \text{tout diviseur commun à } a_1, \dots, a_n \text{ divise } \delta \end{cases}$

Notation 2 : On le note $pgcd(a_1, \dots, a_n)$ ou $a_1 \wedge \dots \wedge a_n$.

Lemme 3 : Deux pgcd de $a_1, \dots, a_n$ sont associés.

Déf 4 : On dit que A est un anneau à pgcd si deux éléments quelconques a, b de A^* admettent un pgcd.

BEN 517

Contre-ex 5 : Dans $\mathbb{Z}[i\sqrt{5}]$, $9 = (2+i\sqrt{5})(2-i\sqrt{5})$ et $3(2+i\sqrt{5})$ n'ont pas de pgcd.

ROM 245

Déf 6 : Soit A un anneau à pgcd. On dit que $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble si leur pgcd est dans $A^\times$.

Théorème 7 : Soit d un diviseur commun à $a_1, \dots, a_n$ et on note alors $a_k = d\, d_k \ \forall k \in [\![1; n]\!]$. On a :
$d = pgcd(a_1, \dots, a_n) \iff pgcd(d_1, \dots, d_n) = 1$

Théorème 8 (de Gauss) : Soit $a, b \in A^*$. Alors a et b sont premiers entre eux ssi $\forall c \in A^*$, $a \mid bc$ entraîne que $a \mid c$.

Déf 9 : On dit que $a_1, \dots, a_n$ admettent un plus petit commun multiple s'il existe $p \in A^*$ tel que :
$\begin{cases} \forall k \in [\![1; n]\!], \ p \text{ est multiple de } a_k \\ \text{tout multiple commun à } a_1, \dots, a_n \text{ est multiple de } p. \end{cases}$

Notation 10 : On le note $ppcm(a_1, \dots, a_n)$ ou $a_1 \vee \dots \vee a_n$.

Lemme 11 : Deux ppcm de $a_1, \dots, a_n$ sont associés.

Prop 12 : Le ppcm et le pgcd sont commutatifs et associatifs.

Théorème 13 : A est un anneau à pgcd ssi tout éléments $a, b \in A^*$ admettent un ppcm. On a alors :
$ab = pgcd(a,b) \times ppcm(a,b)$ à une unité près.

2) Dans un anneau factoriel [ROM]

Déf 14 : On dit que A est factoriel s'il est intègre et si tout élément non nul et non inversible s'écrit de manière unique comme produit d'éléments irréductibles (à permutation et association des facteurs près).

ROM 224

Théorème 15 : Un anneau factoriel A est à pgcd. Plus précisément, pour $a = u \prod_{k=1}^{n} p_k^{m_k}$ et $b = v \prod_{k=1}^{n} p_k^{n_k}$ dans $A^* \setminus A^\times$ où $u, v \in A^\times$, les p_k sont irréductibles deux à deux non associés et $m_k, n_k \in \mathbb{N}$. On a :
$pgcd(a,b) = \prod_{k=1}^{n} p_k^{\min(m_k, n_k)}$.

ROM 244

Prop 16 : Dans un anneau factoriel, pour $\lambda, a_0, \dots, a_n \in A^*$, on a $pgcd(\lambda a_0, \dots, \lambda a_n) = \lambda\, pgcd(a_0, \dots, a_n)$

3) Dans un anneau principal [ROM] [PER] [ULM]

Déf 17 : On dit que A est principal s'il est intègre et si tout idéal de A est principal.

ROM 237

Exemple 18 :
- Un corps est un anneau principal
- $\mathbb{Z}$ est est principal
- $K[X]$ est principal ssi K est un corps.

Prop 19 : Un anneau principal est factoriel. Ainsi tout anneau principal est un anneau à pgcd.

PER 47

Théorème 20 (décomposition de Bézout) : Soit A un anneau principal. Un pgcd d de $a_1, \dots, a_m$ est un générateur de $(a_1, \dots, a_m)$ donc tel que $(d) = (a_1, \dots, a_m)$. Un ppcm b de $a_1, \dots, a_m$ est un générateur de $(a_1) \cap \dots \cap (a_m)$ donc tel que $(b) = (a_1) \cap \dots \cap (a_m)$. En particulier, le pgcd

ULM 42

d de $a_1, \dots, a_m$ dans A est une combinaison linéaire de la forme : $d = b_1 a_1 + \dots + b_m a_m$ avec $b_i \in A$.
Cette relation s'appelle une relation de Bézout.

Corollaire 21 : Soit A principal. Alors $a, b \in A$ sont premiers entre eux ssi il existe $u, v \in A$ tel que $au + bv = 1$

Lemme 22 (d'Euclide et de Gauss) : Soit A principal, $c \in A$, a et b dans A premiers entre eux. Alors :
1) $a \mid bc$ implique que $a \mid c$.
2) $a \mid c$ et $b \mid c$ implique que $ab \mid c$.

FER 49 **Contre-ex 23 :** Le théorème de Bézout n'est pas vrai dans un anneau factoriel non principal. Par exemple dans $\mathbb{Z}[X]$, 2 et X sont premiers entre eux mais $(2) + (X) = (2, X) \neq (1)$.

II Algorithme de calcul dans un anneau euclidien [ULM] [ROM] [GOU]

ULM 43 **Déf 24 :** Un anneau A est dit euclidien s'il est intègre et s'il existe une fonction $v : A^* \to \mathbb{N}$ tel que pour $a \in A$ et $b \in A^*$, il existe $q, r \in A$ tel que $a = bq + r$ avec $r = 0$ ou $v(r) < v(b)$. L'élément q est le quotient et l'élément r le reste de la division. La fonction v est appelé stathme euclidien pour A.

Exemple 25 : L'anneau $\mathbb{Z}$ est euclidien pour $v(n) = |n|$.

Prop 26 : Tout anneau euclidien est principal.

Contre-ex 27 : $\mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$ est principal mais non euclidien.

ULM 47 **Prop 28 :** Soit K un corps. Alors $K[X]$ est euclidien pour le stathme $v(P) = \deg(P)$.

ROM 264 Soit (A, φ) un anneau euclidien.

Lemme 29 : Soit $a, b \in A^*$ et r un reste dans la division euclidienne de a par b. A un inversible près :
- Si $r = 0$, $\text{pgcd}(a, b) = b$
- Sinon, $\text{pgcd}(a, b) = \text{pgcd}(b, r)$

Algorithme 30 (d'Euclide) : Soit $a, b \in A^*$ tel que $\varphi(a) \geq \varphi(b)$.
On définit une suite $(r_n)_{n \geq 0}$ d'éléments de A par :
1) $r_0 = b$
2) r_1 est un reste de la div eucli de a par b. Ainsi $r_1 = 0$ ou $0 \leq \varphi(r_1) < \varphi(r_0)$.
3) Pour $n \geq 2$, si $r_{n-1} = 0$ alors $r_n = 0$. Sinon r_n est un reste dans la div eucli de r_{n-2} par r_{n-1} et on a $r_n = 0$ ou $0 \leq \varphi(r_n) < \varphi(r_{n-1})$.

Il existe alors $p \in \mathbb{N}^*$ tel que $r_p = 0$ et $0 \leq \varphi(r_{p-1}) < \dots < \varphi(r_1) < \varphi(r_0)$ et alors
$\text{pgcd}(a, b) = \text{pgcd}(r_0, r_1) = \dots = \text{pgcd}(r_{p-1}, r_p) = r_{p-1}$
Ainsi $\text{pgcd}(a, b)$ est le dernier reste non nul dans cette suite finie de divisions euclidiennes.

Exemple 31 : On considère les nombres 47 et 111. GOU 12
On a l'algorithme d'Euclide :
$111 = 47 \times 2 + 17$
$47 = 17 \times 2 + 13$ Donc : $\text{pgcd}(47, 111) = 1$
$17 = 13 \times 1 + 4$
$13 = 4 \times 3 + 1$

Application 32 : Soit $P = X^a - 1$ et $Q = X^b - 1$ dans $K[X]$ $a, b \in \mathbb{N}^*$ GOU 60
Alors : $\text{pgcd}(P, Q) = X^{\text{pgcd}(a,b)} - 1$.

Algorithme 33 (d'Euclide étendu) : En revenant à l'algorithme précédent, on peut obtenir une relation de Bézout. ROM 265

Exemple 34 : En reprenant l'exemple 31, on a : GOU 12
$1 = 13 - 4 \times 3 = 13 - (17 - 13) \times 3 = 4 \times 13 - 17 \times 3$
$= 4 \times (47 - 17 \times 2) - 17 \times 3 = 4 \times 47 - 11 \times 17$
$= 4 \times 47 - 11 \times (111 - 47 \times 2) = 26 \times 47 - 11 \times 111$.
Donc $1 = 47u + 111v$ avec $u = 26$ et $v = -11$

III Applications

1) Théorème chinois [ROM]

ROM 249

Soit A un anneau principal.

Lemme 35 : Soit $a_1, \dots, a_n$ des éléments de A deux à deux premiers entre eux. Soit $a = \prod_{j=1}^{n} a_j$ et $b_j = \frac{a}{a_j}$ $\forall j \in [\![1; n]\!]$. Alors les b_j sont premiers entre eux dans leur ensemble.

Théorème 36 (chinois) : Soit $a_1, \dots, a_n$ deux à deux premiers entre eux. Alors l'application $f : A \to \prod_{j=1}^{n} A/(a_j)$, $x \mapsto (\pi_j(x))_{1 \le j \le n}$ est un morphisme d'anneaux surjectif de noyau $\mathrm{Ker}(f) = (a)$. Ainsi f induit un isomorphisme d'anneaux

$\tilde{f} : A/(a) \to \prod_{j=1}^{n} A/(a_j)$ d'inverse $\tilde{f}^{-1} : \prod_{j=1}^{n} A/(a_j) \to A/(a)$,

$(\pi_j(x_j))_{1 \le j \le n} \mapsto \pi\left(\sum_{i=1}^{n} x_i m_i b_i\right)$ où les m_i sont tel que $\sum_{j=1}^{n} m_j b_j = 1$.

ROM 293 288

Application 37 : On appelle indicatrice d'Euler le nombre $\varphi(n)$ d'entiers entre 1 et n premiers avec n. Ainsi $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

Soit $n \ge 2$ et $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ sa décomposition en facteurs premiers. On a :

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

DEV 1

ROM 291

Application 38 : Le système de congruences

$$\begin{cases} k \equiv 2 \ [4] \\ k \equiv 3 \ [5] \\ k \equiv 1 \ [9] \end{cases}$$

admet pour solutions l'ensemble $S = \{ 838 + 180\eta ; \eta \in \mathbb{Z} \}$

2) En algèbre linéaire [MAN][BER]

Soit K un corps et E un K-espace vectoriel de dimension finie $n \ge 1$. Soit $u \in \mathcal{L}(E)$.

MAN 43

Lemme 39 (des noyaux) : Soit $P_1, \dots, P_N$ une famille de polynômes deux à deux premiers entre eux. Alors :

$\mathrm{Ker}(P_1 P_2 \dots P_N)(u) = \bigoplus_{k=1}^{N} \mathrm{Ker}(P_k(u))$. De plus, le projecteur de $\mathrm{Ker}(P_1 P_2 \dots P_N)(u)$ sur l'un de ses sous-espaces parallèlement à la somme des autres appartient à $K[u]$.

BER 944

Déf 40 : L'annulateur de u est $\mathrm{Ann}(u) = \{ P \in K[X] ; P(u) = 0 \}$. C'est un idéal de $K[X]$. Il existe un unique polynôme unitaire $\mu_u \in K[X]$ qui engendre $\mathrm{Ann}(u)$. Il est appelé polynôme minimal de u.

Il s'agit de l'unique polynôme unitaire de $K[X]$ tel que $\forall P \in K[X]$, $P(u) = 0 \iff \mu_u \mid P$.

3) Polynômes [PER]

PER 51

Soit A un anneau factoriel et K son corps des fractions.

Déf 41 : Soit $P \in A[X] \setminus \{0\}$. On définit son contenu, noté $c(P)$, comme un pgcd de ses coefficients

On dit que P est primitif si $c(P) = 1$.

Lemme 42 : On a : $c(PQ) = c(P) \cdot c(Q)$.

Prop 43 : Si $P \in A[X]$ est de degré ≥ 1 et irréductible dans $A[X]$, alors il est primitif et irréductible dans $K[X]$.

PER 76

Théorème 44 (critère d'Eisenstein) : Soit $p(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$. Soit $p \in A$ un élément irréductible tel que :

1) $p \nmid a_n$ 2) $p \mid a_i$ $\forall i \in [\![0; n-1]\!]$ 3) $p^2 \nmid a_0$

Alors P est irréductible dans $K[X]$.

DEV 2

Exemple 45 : En prenant $X^n - 2 \in \mathbb{Z}[X]$ pour $n \ge 1$, il existe des polynômes irréductibles de tout degré dans $\mathbb{Q}[X]$.

∅

PER 77

Application 46 : Soit p un nombre premier. Alors $\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \dots + X + 1$ le p-ième polynôme cyclotomique est irréductible sur $\mathbb{Z}$.