[Rom] [illegible] G 2, 2.46 261
[Ber] S. Ulma
[Per] n°11

142 : PGCD et PPCM, algorithmes de calcul. Applications

I - Notion de PGCD et PPCM

1) Anneau quelconque [Rom] 242-246 [Ber] 533

- def pgcd, anneau à pgcd
- CE $\mathbb{Z}[i\sqrt{5}]$
- def premiers entre eux, lemme de Gauss
- def ppcm
- relation $ab = (a \wedge b)(a \vee b)$

2) Anneau factoriel [Rom] 224

- def
- Th anneau à pgcd

3) Anneau principal [Rom] 227 [Ber] 243 540

- def + ex [Per] 49
- ($\mathbb{Z}$, corps, $K[X]$ ssi $\mathbb{K}$ corps)
- principal ⇒ factoriel
- CE $\mathbb{K}[X,Y]$ pas principal
- Th Bezout
- lemme d'Euclide, Gauss
- CE Bezout pas dans factoriel

II - Algorithme de calcul dans un anneau euclidien

- def euclidien ex $\mathbb{Z}$ [Rom] 261 272 264
- euclidien ⇒ principal [Ber] 546
- CE [G] 12
- Algo d'Euclide ex Gourdon [ULmA] 44
- app Gourdon p12
- Algo d'Euclide étendu ex: Gourdon

III - Applications

1) Théorème des restes chinois [Rom] 249
- def premier entre eux et dans leur ensemble
- Th
- app

DEV1

2) Polynômes [Rom] 282 384
- def contenu
- lemme de Gauss + critère d'Eisenstein
- ex

DEV2

Appuyer sur le contenu de cette leçon

142: PGCD et PPCM, algorithmes de calcul
Applications

I- Notion de PGCD et PPCM

1) Dans un anneau quelconque

Soit A un anneau intègre.

[Rom] 242

Définition 1: Soient $r \in \mathbb{N} \setminus \{0,1\}$ et $a_1, \dots, a_r$ des éléments de A^*. On dit que ces éléments admettent un plus grand commun diviseur s'il existe $\delta \in A^*$ tel que
$\begin{cases} \forall k \in \{1,\dots,r\},\ \delta \text{ divise } a_k \\ \text{tout diviseur commun à } a_1,\dots,a_r \text{ divise } \delta \end{cases}$

Définition 2: On dit que l'anneau A est un anneau à pgcd si deux éléments quelconque a, b de A^* admettent un pgcd.

Per 533

Contre exemple 3: $A = \mathbb{Z}[i\sqrt{5}]$ n'est pas un anneau à pgcd. 9 et $3(2+i\sqrt{5})$ n'ont pas de pgcd.

Rom 245

Définition 4: Soient $r \in \mathbb{N} \setminus \{0,1\}$ et $a_1, \dots, a_r$ des éléments tous non nuls dans un anneau à pgcd A. On dit que $a_1, \dots, a_r$ sont premiers entre eux dans leur ensemble si leur pgcd est dans $A^\times$.

Lemme 5 (Gauss): Deux éléments non nuls a, b d'un anneau à pgcd A sont premiers entre eux si, et seulement si, pour tout $c \in A^*$, a divise bc entraine a divise c.

Définition 6: Soient $r \in \mathbb{N} \setminus \{0,1\}$ et $a_1, \dots, a_r$ des éléments de A^*. On dit que ces éléments admettent un plus petit commun multiple s'il existe $\mu \in A^*$ tel que
$\begin{cases} \forall k \in \{1,\dots,r\},\ \mu \text{ est multiple de } a_k \\ \text{tout multiple commun à } a_1,\dots,a_r \text{ est multiple de } \delta. \end{cases}$

Théorème 7: L'anneau A est à pgcd si et seulement si, deux éléments quelconque $a, b \in A^*$ admettent un ppcm. Dans ce cas, on a $ab = \text{pgcd}(a,b)\,\text{ppcm}(a,b)$ à l'unité près. 246

Notation: $a \wedge b := \text{pgcd}(a,b)$ $\quad a \vee b = \text{ppcm}(a,b)$

2) Anneau factoriel

Définition 8: On dit que A est factoriel, s'il est intègre et si tout élément a non nul et non inversible s'écrit de manière unique comme produit d'éléments irréductibles (à ordre des facteurs et multiplication par un inversible près) 220

Théorème 9: Un anneau factoriel A est à pgcd. Plus précisément, pour $a = u \prod_{k=1}^{r} p_k^{m_k}$ $\quad b = v \prod_{k=1}^{r} p_k^{n_k}$ dans $A^* \setminus A^\times$ où u et v sont inversibles, les p_k irréductibles deux à deux non associés et les n_k, m_k des entiers naturels. On a : $a \wedge b = \prod_{k=1}^{r} p_k^{\min(n_k, m_k)}$

3) Anneau principal

Définition 10: On dit que l'anneau A est principal s'il est intègre et si tout idéal de A est principal

Exemple 11 : Un corps est un anneau principal. (ses seuls idéaux sont (0) et (1).
• $\mathbb{Z}$, $\mathbb{K}[X]$ ($\mathbb{K}$ corps), $\mathbb{Z}[i]$ sont principaux

227 **Proposition 12 :** Un anneau principal est factoriel

Contre exemple 13 : $\mathbb{K}[X,Y]$ pas principal mais factoriel

Théorème 14 : Un anneau principal A est un anneau à pgcd. Pour toute famille $\{a_1,\dots,a_r\}$ de $r \geq 2$ éléments de A^*, il existe $\delta \in A^*$ tel que $(a_1,\dots,a_r)=(\delta)$ et $\delta = \sum_{k=1}^{r} u_k a_k$ $u_i \in A$ $\forall i \in [\![1,r]\!]$

Per 243

et $\delta = \text{pgcd}(a_1,\dots,a_r)$

Théorème 15 : (Bezout) Soient $r \in \mathbb{N}\setminus\{0,1\}$ et $a_1,\dots,a_r$ des éléments tous non nuls dans A principal. Ces éléments sont premiers entre eux dans leur ensemble si et seulement si, il existe $(u_1,\dots,u_r) \in A^r$ tels que $\sum_{k=1}^{r} u_k a_k = 1$

Lemme 16 (Gauss) Soit A anneau principal.

Ber 540

Soient $a,b \in A$, $a \wedge b = 1$. Alors $\forall c \in A$ $a \mid bc \Rightarrow a \mid c$.

Lemme 17 (Euclide) : Soit A anneau principal. Soit $a,b \in A$ $a \wedge b = 1$. Alors $a \mid c$ et $b \mid c \Rightarrow ab \mid c$

Contre exemple : 18 Bezout est en défaut dans un anneau factoriel non principal.

[Per] p49

Exemple : $K[X,Y]$

II – Algorithme de calcul dans un anneau euclidien

Définition 19 : Un anneau commutatif et intègre A est dit euclidien, s'il existe un stathme $\varphi : A^* \to \mathbb{N}$ tel que $\forall (a,b) \in A^2$, $b \neq 0_A$, il existe $(q,r) \in A^2$ tel que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$

[Ram] 261

Exemple 20 : • $\mathbb{Z}$ est euclidien (pour $|\cdot|$)

[Per] 346

• $\mathbb{K}[X]$ euclidien pour le degré (avec $\mathbb{K}$ corps)

Proposition 21 : Euclidien $\Rightarrow$ principal

[Ram] 261

Exemple 22 : $\mathbb{Z}\left[\frac{1}{2}(1+i\sqrt{19})\right]$ est principal mais pas euclidien

272

Lemme 23 : Soient $a,b \in A^*$ un anneau euclidien et r un reste de la division euclidienne de a par b. On a alors $a \wedge b = b$ si $r = 0_A$ ou $a \wedge b = b \wedge r$ si $r \neq 0_A$

264

Algorithme d'Euclide 24 : Soient $a,b \in A^*$ tels que $\varphi(a) \geq \varphi(b)$. On pose $r_0 = b$ et on désigne par r_1 un reste dans la division euclidienne de a par b. On pose $r_{-1} = a$. Pour $n \geq 1$ on définit r_n comme le reste de la division euclidienne de r_{n-2} par r_{n-1}. Comme $0 \leq \varphi(r_{p-1}) < \dots < \varphi(r_1) < \varphi(r_0)$, il existe $N \in \mathbb{N}$ tel que $r_N = 0$ et $a \wedge b = r_0 \wedge r_1 = \dots = r_{N-1} \wedge r_N = r_{N-1}$

TN-1 G-12

Exemple 25 : On a $47u + 111v = 1$ avec $u = 26$ $v = -11$

Algorithme d'Euclide étendu 26 : Soient $a,b \in A^*$ tels que $\varphi(a) \geq \varphi(b)$. On cherche $d = \text{pgcd}(a,b)$ et une relation de Bezout $d = au + bv$.

[CLMA] p44

	$r_0 = a = 1 \cdot a + 0 \cdot b$ $r_1 = b = 0 \cdot a + 1 \cdot b$
$r_0 - q_1 r_1 =$	$r_2 =$ $1 \cdot a + (-q_1) \cdot b$
$\vdots$	
$r_{i-1} - q_i r_i =$	$r_{i+1} =$ $u_{i+1} \cdot a + v_{i+1} b$
$\vdots$	
$r_{n-2} - q_{n-1} r_{n-1} =$	$r_n =$ $u_n \cdot a + v_n \cdot b$
$r_{n-1} - q_n r_n =$	$0 =$ $u_{n+1} \cdot a + v_{n+1} b$
euclide	$\exists n$ avec $r_{n+2} = 0$

III- Applications

1) Théorème des restes chinois

[Rom] 249

Théorème 27: Soient $n_1, \dots, n_r \in \mathbb{N}$ deux à deux premiers entre eux, alors

$$\mathbb{Z}/n_1 \cdots n_r \mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

DEV 1

Application 28:

On considère le système suivant:

$$\begin{cases} u \equiv 1 \ [3] \\ u \equiv 3 \ [5] \\ u \equiv 0 \ [7] \end{cases}$$

Les solutions dans $\mathbb{Z}$ sont de la forme $28 + 105k$ $k \in \mathbb{Z}$

2) Polynômes

Définition 29: Le contenu de $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$ (avec A un anneau) est l'entier 382

$$c(P) = \text{pgcd}(a_0, a_1, \dots, a_n)$$

On dit qu'un polynôme $P \in A[X]$ non nul est primitif si son contenu vaut 1.

Lemme 30 (Gauss) Pour $P, Q \in A[X]$ on a 384

$$c(PQ) = c(P)c(Q)$$

DEV 2

Théorème 31: (Eisenstein)

Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$ avec A un anneau factoriel et $K = \text{Frac}(A)$ corps.

Soit $p \in A$ irréductible tel que:

- p divise $a_0, \dots, a_{n-1}$
- p ne divise pas a_n
- p^2 ne divise pas a_0

Alors P irréductible dans $K[X]$. Si de plus P primitif alors P irréductible dans $A[X]$

But: Généraliser les notions de pgcd, ppcm connues dans $\mathbb{Z}$ à d'autres anneaux

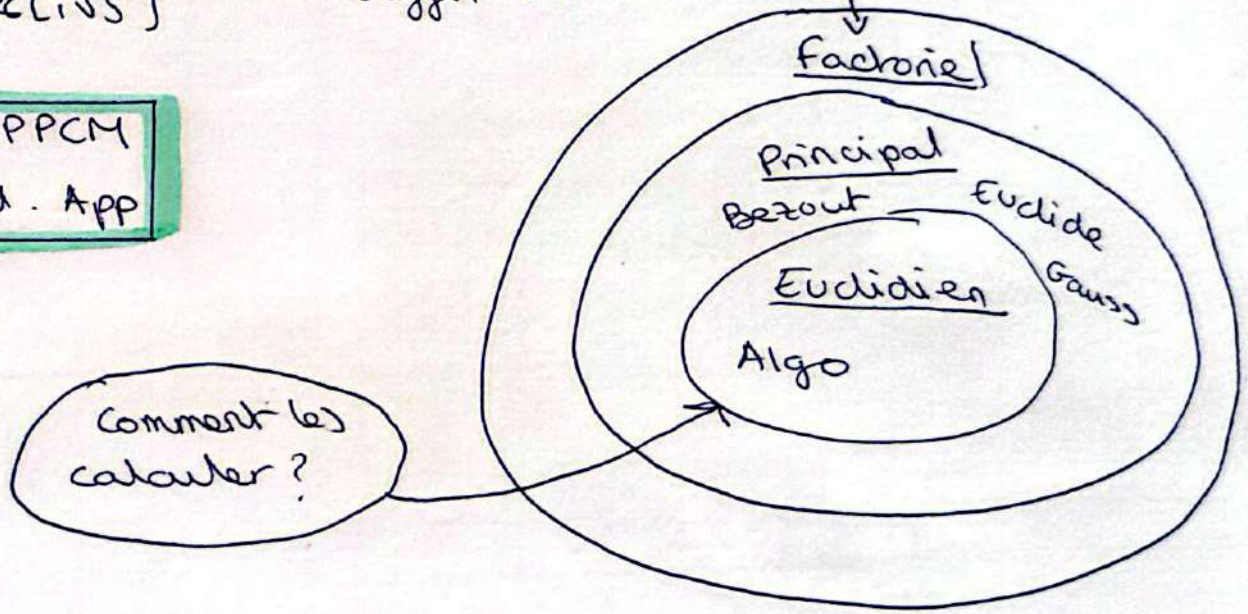
} Dans quels cadres peut-on affirmer l'existence ?

⚠ Tt les anneaux ne sont pas à pgcd ex $\mathbb{Z}[i\sqrt{5}]$

↳ anneau factoriel suffit

cas le + général

142: PGCD PPCM
algo de calcul. App



⚠ pgcd ppcm unique à inversible près

Application

Th restes chinois

$\mathbb{Z}/n_1 \cdots n_r\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$

irréductibilité polynôme

↳ critère d'Eisenstein

CONTENU ⚠