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

Références : Rombaldi, Perrin, Gourdon (Dunford), Berhuy (exposant), Demazure

## I - Notion de PGCD et PPCM dans différents types d'anneaux

### 1) Définitions et premières propriétés
### 2) Cas des anneaux factoriels
### 3) Cas des anneaux principaux

## II - Algorithmes de calcul dans un anneau euclidien

### 1) Algorithme d'Euclide : mise en place
### 2) Coût de l'algorithme d'Euclide dans $\mathbb{Z}$ et $K[X]$

## III - Applications

### 1) Décomposition de Dunford
### 2) Résolution d'équations diophantiennes et théorème chinois
### 3) Arithmétique en théorie des groupes

DEV 1 : Irréductibilité de $\Phi_n$ (avec lemme de Gauss)

DEV 2 : Décomposition de Dunford

# Leçon 142 : PGCD et PPCM. Algorithmes de calcul. Applications

Soit $A$ un anneau commutatif unitaire intègre

## I - Notion de PGCD et PPCM dans différents types d'anneaux

### 1) Définitions et premières propriétés [Ran]

**DEF 1** : Soient $n \in \mathbb{N}$, $n \geq 2$ et $a_1, \dots, a_n$ des éléments de $A \setminus \{0\}$. On dit que ces éléments admettent un plus grand commun diviseur (PGCD) lorsqu'il existe $\delta \in A \setminus \{0\}$ tel que :
- $\forall k \in [\![1;n]\!]$, $\delta \mid a_k$
- Tout diviseur commun à $a_1, \dots, a_n$ divise $\delta$

**LEMME 2** : Deux PGCD d'une famille $\{a_1, \dots, a_n\}$ d'éléments de $A \setminus \{0\}$ sont associés.

**DEF 3** : Soient $n \in \mathbb{N}$, $n \geq 2$ et $a_1, \dots, a_n$ dans $A \setminus \{0\}$. On dit que $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble (ou étrangers) lorsque leur PGCD est dans $A^\times$.

**DEF 4** : Soient $n \in \mathbb{N}$, $n \geq 2$ et $a_1, \dots, a_n$ dans $A \setminus \{0\}$. On dit que ces éléments admettent un plus petit commun multiple lorsqu'il existe $\mu \in A \setminus \{0\}$ tel que :
- $\forall k \in [\![1,n]\!]$, $a_k \mid \mu$
- Tout multiple commun à $a_1, \dots, a_n$ est multiple de $\mu$

**LEMME 5** : Deux PPCM de $\{a_1, \dots, a_n\}$ sont associés.

**THM 6** : Soient $a, b \in A \setminus \{0\}$. Alors $a$ et $b$ admettent un PGCD si et seulement s'ils admettent un PPCM. Dans ce cas, on a $ab = \mathrm{PGCD}(a,b)\,\mathrm{PPCM}(a,b)$ (à un inversible près).

**THM 7** : Soient $n \in \mathbb{N}$, $n \geq 2$, $a_1, \dots, a_n$ dans $A \setminus \{0\}$ admettant un PGCD. Soit $d$ un diviseur commun à $a_1, \dots, a_n$. $\forall k \in [\![1,n]\!]$, $a_k = d\alpha_k$. On a alors :
$$d = \mathrm{PGCD}(a_1, \dots, a_n) \iff \mathrm{PGCD}(\alpha_1, \dots, \alpha_k) = 1.$$

### 2) Cas des anneaux factoriels [PER] (Ran)

**DEF 8** : On dit que $A$ est factoriel lorsqu'il est intègre et :
(E) Tout élément $a \in A \setminus \{0\}$ s'écrit $a = u p_1 \cdots p_r$, $u \in A^\times$ et $p_1, \dots, p_r$ irréductibles.
(U) Cette décomposition est unique à permutation et à inversibles près : si $a = u p_1 \cdots p_r = v q_1 \cdots q_s$, alors $r = s$ et il existe $\sigma \in \mathfrak{S}_n$ tel que $p_i = q_{\sigma(i)}$. On écrit $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$.

**PROP 9** : Soit $A$ intègre vérifiant (E). LASSE :
1) $A$ vérifie (U)
2) Lemme d'Euclide : si $p$ est irréductible et $p \mid ab$, alors $p \mid a$ ou $p \mid b$.
3) $p$ irréductible $\Leftrightarrow (p)$ est premier
4) Gauss : si $a \mid bc$ et $a$ est premier avec $b$, alors $a \mid c$.

Dans la suite, $A$ est factoriel.

**THM 10** : Soit $a = u \prod_{k=1}^{n} p_k^{m_k}$ et $b = v \prod_{k=1}^{n} p_k^{m_k}$ dans $(A \setminus \{0\}) \setminus A^\times$ où $u, v \in A^\times$, $p_k$ irréductibles deux à deux non associés, $m_k, m_k \in \mathbb{N}$. On a $\mathrm{PGCD}(a,b) = \prod_{k=1}^{n} p_k^{\min(m_k; m_k)}$ et $\mathrm{PPCM}(a,b) = \prod_{k=1}^{n} p_k^{\max(m_k; m_k)}$

**REM 11** : On déduit que dans un anneau factoriel, pour tous $\lambda, a_1, \dots, a_n$ dans $A \setminus \{0\}$, $\mathrm{PGCD}(\lambda a_1, \dots, \lambda a_n) = \lambda\,\mathrm{PGCD}(a_1, \dots, a_n)$

**REM 12** : Dans un anneau non factoriel, deux éléments peuvent ne pas admettre de PGCD ou de PPCM : dans $\mathbb{Z}[i\sqrt{5}]$ 9 et $3(2+i\sqrt{5})$ n'ont pas de PGCD ; 3 et $2+i\sqrt{5}$ n'ont pas de PPCM

**DEF 13** : Pour $P \in A[X]$, $P \neq 0$, on définit le contenu de $P$, noté $c(P)$ : si $P(X) = a_n X^n + \cdots + a_0$, $c(P) = \mathrm{PGCD}(a_0, \dots, a_n)$ (modulo $A^\times$). $P$ est dit primitif lorsque $c(P) = 1$. DEV 1

**LEMME 14** (Gauss) On a $c(PQ) = c(P)c(Q)$ modulo $A^\times$.

**PROP 15** : Soient $A, P, B \in \mathbb{Q}[X]$. On suppose $A, P$ unitaires, $P \in \mathbb{Z}[X]$ et $P = AB$. Alors $A, B \in \mathbb{Z}[X]$.

**APPLI 16** : $\forall n \in \mathbb{N}^*$, $\Phi_n$ est irréductible dans $\mathbb{Q}[X]$.

### 3) Cas des anneaux principaux [Ran] [PER]

**DEF 17** : $A$ est dit principal lorsqu'il est intègre et que tous ses idéaux sont principaux.

**PROP 18** : Un anneau principal est factoriel donc on peut définir la notion de PGCD dans $A$.

**PROP 19** : Soit $A$ principal et $a_1, \dots, a_n$ dans $A \setminus \{0\}$. Soit $d = \mathrm{PGCD}(a_1, \dots, a_n)$. Alors $(d) = (a_1) + (a_2) + \cdots + (a_n)$ i.e. : $\exists \lambda_1, \dots, \lambda_n \in A$, $d = \sum_{k=1}^{n} \lambda_k a_k$. Une telle relation s'appelle relation de Bezout.

**COR 20** : Soit $A$ principal et $a, b \in A \setminus \{0\}$. Alors $a$ et $b$ sont premiers entre eux si et seulement si : $\exists \lambda, \mu \in A$, $1 = \lambda a + \mu b$.

REM 21: Le théorème précédent (de Bezout) est en défaut dans un anneau factoriel non principal : $K[X,Y]$ est factoriel et $X$ et $Y$ sont premiers entre eux mais on a $(X)+(Y)=(X,Y)\neq(1)$.

## II - Algorithmes de calcul dans un anneau euclidien

### 1) Algorithme d'Euclide : mise en place [PEF] [Rost]

DEF 22: $A$ est dit euclidien lorsqu'il est intègre et lorsque $A^*$ est muni d'une division euclidienne c'est-à-dire :
$\exists v : A\setminus\{0\} \to \mathbb{N}$ telle que $\forall (a,b)\in A\times A\setminus\{0\}$, $\exists q,r\in A$,
$\begin{cases} a=bq+r \\ r=0 \text{ ou } v(r)<v(b) \end{cases}$

EX 23: $\mathbb{Z}$ et $K[X]$ sont euclidiens ($K$ un corps)

THM 24: Un anneau euclidien est principal.

Dans la suite, on suppose $A$ euclidien.

LEMME 25: Soient $a,b\in A\setminus\{0\}$ et $r$ un reste dans la division euclidienne de $a$ par $b$. On a alors : $PGCD(a,b)=b$ si $r=0$ ou $PGCD(a,b)=PGCD(b,r)$ sinon (à un inversible près)

ALGORITHME 26: Soit $a,b\in A\setminus\{0\}$, $v(b)\leq v(a)$. On note $r_i$ un reste dans la division euclidienne de $a$ par $b$. Si $r_1=0$, $PGCD(a,b)=b$, sinon, $v(r_1)<v(r_0)$ et on a $PGCD(a,b)=PGCD(r_0,r_1)$. On désigne alors par $r_2$ un reste dans la division euclidienne de $r_0$ par $r_1$. Si $r_2=0$, $PGCD(a,b)=r_1$, sinon on continue avec $PGCD(r_0,r_1)=PGCD(r_1,r_2)$. On définit alors $(r_n)_{n\in\mathbb{N}}\in A^{\mathbb{N}}$ par :
- $r_0=b$
- $r_1$ est un reste dans la division euclidienne de $a$ par $b$ : $r_1=0$ ou $0\leq v(r_1)<v(r_0)$
- Pour $n\geq 2$, $r_{n-1}=0 \Rightarrow r_n=0$, sinon $r_n$ est un reste de la division euclidienne de $r_{n-2}$ par $r_{n-1}$ et on a $r_n=0$ ou $0\leq v(r_n)<v(r_{n-1})$.

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

On a en fait construit avec l'algorithme d'Euclide, dans le cas où $b\nmid a$, deux suites $(r_n)_{0\leq n\leq p}$ et $(q_n)_{1\leq n\leq p}$ d'éléments de $A$ de la manière suivante :

$$\begin{cases} a=q_1r_0+r_1 & (r_1\neq 0,\ v(r_1)<v(r_0)) \\ r_0=q_2r_1+r_2 & (r_2\neq 0,\ v(r_2)<v(r_1)) \\ r_{p-3}=q_{p-1}r_{p-2}+r_{p-1} & (r_{p-1}\neq 0 \text{ et } v(r_{p-1})<v(r_{p-2})) \\ r_{p-2}=q_pr_{p-1}+r_p & (r_p=0). \end{cases}$$

ALGORITHME 27 (Euclide étendu) On vérifie alors qu'il existe $u_k$ et $v_k$ dans $A$ tels que $r_k=au_k+bv_k$. $k=0$ et $k=1$, $r_0=b=a\cdot 0+b\cdot 1$ et $r_1=a\times 1+b(-q_1)$. En supposant le résultat acquis jusqu'à $k-1$, $0\leq k-1\leq p-2$,

$$r_k=-q_kr_{k-1}+r_{k-2}=-q_k(au_{k-1}+bv_{k-1})+au_{k-2}+bv_{k-2}$$
$$=a(u_{k-2}-q_ku_{k-1})+b(v_{k-2}-q_kv_{k-1})=au_k+bv_k$$

APPLI 28: On a $\mathbb{F}_9\simeq \mathbb{F}_3[X]/(X^2+1)$. Soit $\alpha=\overline{X}$. L'inverse de $1+\alpha$ dans $\mathbb{F}_9$ est $\alpha-1$. [DEF 2.2.6]

### 2) Coût de l'algorithme d'Euclide dans $\mathbb{Z}$ et $K[X]$

PROP 29 (Lamé) Soient $x,y$ deux entiers, $0<y<x$ et soit $d$ leur PGCD. Si l'algorithme d'Euclide partant de $(x,y)$ s'arrête au bout de $n$ pas, alors $x\geq dF_{n+2}$ et $y\geq dF_{n+1}$ où $(F_n)$ est la suite de Fibonacci.

COR 30: Soient $x,y$ entiers, $0\leq y\leq x$. L'algorithme d'Euclide calculant $PGCD(x,y)$ prend au plus $\frac{3}{2}\log(y)+1$ pas.

PROP 31: Soit $N$ un entier majorant $x$ et $y$. Le coût de l'algorithme d'Euclide étendu est majoré par $cln(N)^2$ où $c\in\mathbb{N}$.

PROP 32: L'algorithme d'Euclide étendu sur $P$ et $Q$ dans $K[X]$ s'arrête en au plus $n$ étapes lorsque $n\Rightarrow \deg(P)\geq\deg(Q)\geq 1$.

## III - Applications

### 1) Décomposition de Dunford [GOU]

Soit $E$ un espace vectoriel de dimension finie $n \in \mathbb{N}^*$ sur un corps commutatif $K$.

DEV 2

**PROP 33:** Soit $u \in \mathcal{L}(E)$ et $P \in K[X]$, $P = \beta M_1^{\alpha_1} \cdots M_s^{\alpha_s}$ tel que $P(u) = 0$. Pour tout $i \in [\![1; s]\!]$, on note $N_i = \ker(M_i^{\alpha_i}(u))$. On a alors $E = N_1 \oplus \cdots \oplus N_s$ et pour tout $i$, la projection sur $N_i$ parallèlement à $\bigoplus_{j \neq i} N_j$ est un polynôme en $u$.

**THM 34: (Dunford)** Soit $u \in \mathcal{L}(E)$ tel que $\chi_u$ est scindé sur $K$. Il existe un unique couple $(d, n)$ d'endomorphismes tel que (i) $d$ est diagonalisable, $n$ est nilpotent (ii) $u = d + n$ et $d \circ n = n \circ d$. De plus, $d$ et $n$ sont des polynômes en $u$.

**REM 35:** On peut calculer les projecteurs spectraux de $u$ en décomposant $\frac{1}{P}$ en éléments simples avec $P(u) = 0$.

### 2) Résolution d'équations diophantiennes et théorème chinois [ROM]

**DEF 36:** On appelle équation diophantienne toute équation polynomiale à coefficients dans $\mathbb{Z}$ et à solutions entières.

**EX 37:** Pour $a, b \in \mathbb{Z}$, l'équation $ax + by = d$, $d = \text{pgcd}(a, b)$

**PROP 38:** L'équation $ax \equiv 1 \bmod n$ a des solutions si et seulement $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si $a$ est premier avec $n$.

**REM 39:** Dans ce cas, l'algorithme d'Euclide étendu permet de trouver une solution $x_0 \in \mathbb{Z}$.

**PROP 40:** L'ensemble des solutions de $ax \equiv 1 \bmod n$ dans le cas où $\text{PGCD}(a, n) = 1$ est $\{x_0 + kn / k \in \mathbb{Z}\}$.

**THM 41:** L'équation diophantienne $ax \equiv b \bmod n$ a des solutions entières si et seulement si $\text{PGCD}(a, n) \mid b$. Dans ce cas, l'ensemble des solutions est $S = \{\delta b' x_0' + k n' / k \in \mathbb{Z}\}$ où $x_0'$ est une solution particulière de $a'x \equiv 1 \bmod n'$, $a = \delta a'$, $n = \delta n'$, $b = \delta b'$, $\delta = \text{PGCD}(a, n)$.

**THM 42:** (d'isomorphisme chinois) Soit $A$ un anneau principal, $a_1, \ldots, a_n \in A$ deux à deux étrangers, alors

$$A/(a_1 \cdots a_n) \simeq A/(a_1) \times \cdots \times A/(a_n).$$

**APPLI 43:** Le théorème est utilisé pour résoudre des systèmes de congruences de la forme

$$\begin{cases} x \equiv x_1 \bmod n_1 \\ \vdots \\ x \equiv x_n \bmod n_n \end{cases}$$

avec les $n_i$ deux à deux premiers entre eux.

**EX 44:** Les solutions de $\begin{cases} k \equiv 2 \bmod 4 \\ k \equiv 3 \bmod 5 \\ k \equiv 1 \bmod 9 \end{cases}$ sont les $k = 118 + 180q'$, $q' \in \mathbb{Z}$.

### 3) Arithmétique en théorie des groupes [BERH.]

**REM 45:** Certains résultats fondamentaux de théorie des groupes amènent à des raisonnements arithmétiques comme le théorème de Lagrange, la relation orbite-stabilisateur ou l'équation aux classes.

**DEF 46:** On dit que $G$ un groupe est d'exposant fini lorsqu'il existe $n \in \mathbb{N}^*$, $x^n = e_G$ pour tout $x \in G$. Le plus petit entier vérifiant cela est appelé exposant de $G$.

**LEMME 47:** On suppose $G$ d'exposant fini. Alors on a : $\exp(G) = \text{ppcm}(o(x), x \in G)$ et si $G$ est fini, $\exp(G) \mid \#G$.

**EX 48:** Si $G$ est cyclique d'ordre $n$, $\exp(G) = n$ $\exp(\mathfrak{S}_3) = 6$.

**PROP 49:** On suppose $G$ abélien d'exposant fini. Alors il existe $x \in G$ d'ordre $\exp(G)$

**COR 50:** On suppose $G$ abélien fini. $G$ est cyclique si et seulement si $\exp(G) = \#G$.

**THM 51:** Soit $K$ un corps. Tout sous-groupe fini de $K^\times$ est cyclique.

**COR 52:** Soit $p$ premier. Alors $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique et de même tout sous-groupe de $\mathbb{F}_q^*$ est cyclique.