PGCD, PPCM, Algorithme d'Euclide, Applications

Cadre : $A$ est un anneau commutatif, intègre, $a, b \in A$, $\mathbb{K}$ est un corps

# I - Cadre théorique : Anneau quelconque ou factoriel

## 1 - Cas d'un anneau quelconque

**Déf 1 :** (i) $d \in A$ est un PGCD de $a, b \in A$ si $d \mid a$ et $d \mid b$ et si $\forall d' \in A$ tel que $d' \mid a$, $d' \mid b$, alors $d' \mid d$.

(ii) $m \in A$ est un PPCM de $a, b \in A$ si $a \mid m$ et $b \mid m$ et si $\forall m' \in A$ tel que $a \mid m'$ et $b \mid m'$, alors $m \mid m'$.

**Ex 2 :** Dans $\mathbb{Z}$, $2$ est un PGCD de $4$ et $6$.

Dans $\mathbb{Z}[i\sqrt{5}]$, $6$ et $2+2i\sqrt{5}$ n'ont pas de PGCD (car $2$ et $1+i(\overline{5})$ ne divisent pas $6$ et $2+2i\sqrt{5}$).

Dans $\frac{\mathbb{C}[X,Y,Z,T]}{\langle XT - ZT \rangle}$, $\overline{X}$ et $\overline{Z}$ n'ont pas de PPCM (car $\overline{X}\overline{Z}$ et $\overline{Y}\overline{T} = \overline{Z}\overline{T}$).

**Prop 3 :** Un PGCD et un PPCM est unique à multiplication par un inversible près.

**Rq 4 :** On note $a \wedge b$ (« $\wedge$ ») un PGCD de $a$ et $b$, et on note $a \vee b$ (« $\vee$ ») un PPCM de $a$ et $b$ lorsqu'ils sont définis.

**Prop 5 :** Le PGCD et le PPCM sont associatifs (lorsqu'ils sont définis).

Soient $a, b, c \in A$. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ et $(a \vee b) \vee c = a \vee (b \vee c)$.

**Prop 6 :** Soit $c \in A$. Si $(ca) \wedge (cb)$ existe alors $a \wedge b$ aussi et $(ca) \wedge (cb) = c(a \wedge b)$.

**Prop 7 :** Si $a \vee b$ existe alors $a \wedge b$ aussi et $(a \vee b)(a \wedge b) = ab$.

**Rq 8 :** La réciproque n'est pas toujours vraie.

**Ex 9 :** Dans $\frac{\mathbb{C}[X,Y,Z,T]}{\langle XY - ZT \rangle}$, $\overline{X}$ et $\overline{Z}$ sont un PGCD ($\overline{X}\overline{Z} = -1$) mais pas de PPCM.

## 2 - Dans un anneau factoriel

**Déf 10 :** Un anneau $A$ intègre est dit factoriel si il existe un ensemble $\mathrm{Irr}(A)$ d'éléments irréductibles de $A$ (i.e. $a \in \mathrm{Irr}(A) \iff a = a_1 a_2 \Rightarrow a_1 \in A^\times$ ou $a_2 \in A^\times$) tel que : $\forall a \in A$,

$$a = u \prod_{p \in \mathrm{Irr}(A)} p^{\alpha_p}, \quad u \in A^\times, \quad \alpha_p \in \mathbb{N}$$

L'écriture d'un tel produit à permutation près des facteurs $p$ est appelée la valuation de $p$ : On note $\alpha_p = v_p(a)$.

**Prop 11 :** Si $A$ est factoriel alors $a \vee b$ et $a \wedge b$ existent et $\forall a, b \in A$ :

(i) $a \wedge b = \prod_{p \in \mathrm{Irr}(A)} p^{\min(v_p(a), v_p(b))}$

(ii) $a \vee b = \prod_{p \in \mathrm{Irr}(A)} p^{\max(v_p(a), v_p(b))}$

(à multiplication par un inversible près)

**Déf 12 :** On dit que $a$ et $b$ sont premiers entre eux si $a \wedge b = 1$ et autrement si $a \wedge b \neq 1$.

**Ex 13 :** Dans $\mathbb{C}[X]$, $X^2+1 \wedge X+1 = 1 \Rightarrow X^2+1$ et $X+1$ sont premiers entre eux.

**Prop 13-bis :** $\forall a, b \in A$, $a \wedge b = (a+b) \wedge b$ ($A$ factoriel).

**Déf 14 :** Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. On appelle contenu de $P$ : $c(P) = a_1 \wedge \dots \wedge a_n$. $P$ primitif $\iff c(P) = 1$.

**Prop 14-bis :** $\forall P, Q \in A[X]$, $c(PQ) = c(P)c(Q)$.

**Déf 15-bis :** Soit $P \in A[X]$, $d^\circ P \geq 1$. $P \in \mathrm{Irr}(A[X]) \iff c(P) = 1$ et $P \in \mathrm{Irr}(\mathrm{Frac}(A))$.

# II - Cadre effectif : anneau principal ou euclidien

## 1 - Cas d'un anneau principal

**Déf 15 :** Un anneau intègre $A$ est dit principal si tout idéal $I \subset A$ est de la forme $I = \langle a \rangle$, $a \in A$.

**Prop 15-bis :** Si $A$ est principal alors $A$ est factoriel.

**Prop 16 :** Dans un anneau principal $A$, on a, $\forall a, b \in A$ :

(i) $\langle a \rangle + \langle b \rangle = \langle a \wedge b \rangle$

(ii) $\langle a \rangle \cap \langle b \rangle = \langle a \vee b \rangle$

**Ex 17 :** Si $A = \mathbb{Z}$ on a :

- $9\mathbb{Z} + 24\mathbb{Z} = 3\mathbb{Z}$ ($9 \wedge 24 = 3$)
- $3\mathbb{Z} \cap 7\mathbb{Z} = 21\mathbb{Z}$ ($3 \vee 7 = 21$)

**Th 18 :** (Théorème de Bachet-Bézout) Soit $a, b \in A$, $A$ principal.

(i) Si $d = a \wedge b$, $\exists u, v \in A$ : $au + bv = d$.

(ii) $a \wedge b = 1 \iff \exists u, v \in A$ : $au + bv = 1$.

**Th 19 :** (Théorème chinois)

Si $a \wedge b = 1$, alors $\frac{A}{\langle ab \rangle} \simeq \frac{A}{\langle a \rangle} \times \frac{A}{\langle b \rangle}$

## 2 - Cas d'un anneau euclidien

**Déf 20** (Anneau euclidien)
Un anneau intègre $A$ est dit euclidien s'il existe une application $\nu : A\setminus\{0\} \to \mathbb{N}$ appelée stathme euclidien vérifiant : $\forall a, b \in A$

(i) Stab $b \mid a$

(ii) Stab $a = bq + r$ avec $\nu(r) < \nu(b)$

**Prop 21** (Trois exemples d'anneaux euclidiens)

(i) $\mathbb{Z}$ avec $\nu(z) = |z|$ (valeur absolue)

(ii) $\mathbb{Z}[i]$ avec $\nu(z) = |z|^2$ (stathme de la norme)

(iii) $\mathbb{K}[X]$ avec $\nu(P) = \deg(P)$ ($\mathbb{K}$ est un corps, stathme du degré)

**Prop 22** (Algorithme d'Euclide)
Soient $A$ un anneau euclidien, soient $a, b \in A\setminus\{0\}$ avec $\nu(a) \geq \nu(b)$
On note $(r_i)$ la suite définie par $r_0 = b$, $r_1 = a$ et $r_{i+2} = r_i - r_{i+1}\, q_{i+1}$ où $q_{i+1}$ est le quotient de la division euclidienne de $r_i$ par $r_{i+1}$ ($\nu(r_{i+1}) < \nu(r_i)$)
Alors il existe un rang $n_0$ tel que $r_{n_0+1} = 0$ et $r_{n_0} \neq 0$. On a :
$a \wedge b = r_{n_0}$ et $(\nu(r_n))_{n \leq n_0}$ est décroissante strictement de limite nulle.

**Ex 23 :** Donc $\mathbb{Z}$, on a $114 \wedge 76 = 38$
En effet
- $114 = 1 \times 76 + 38$ Dernier reste non nul
- $76 = 2 \times 38 + 0$

**Rq 24 :** On peut aussi calculer un pgcd dans tout anneau euclidien, exemple $\mathbb{Z}$, $\mathbb{Z}[i]$ ou $\mathbb{K}[X]$ ($\mathbb{K}$ est un corps)

**Prop 24 bis :** Soit $(F_n)$ la suite de Fibonacci ($F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$)
Si $\nu(a) \geq \nu(b) \geq 1$ et $\nu(b) < F_{n+1}$, alors l'algorithme d'Euclide pour calculer $a \wedge b$ réalise au plus $n$ appels récursifs

**Prop 25** (Algorithme d'Euclide étendu)
Soient $a, b \in A$, $A$ euclidien. Posons $w_0 = \begin{bmatrix} a \\ 1 \\ 0 \end{bmatrix}$, $w_1 = \begin{bmatrix} b \\ 0 \\ 1 \end{bmatrix}$ avec $\nu(a) \geq \nu(b) \geq 1$

$w_i = \begin{bmatrix} r_i \\ u_i \\ v_i \end{bmatrix}$, $i \in \mathbb{N}^*$ où $(r_i)$ est telle que $r_i = q_{i+2} r_{i+1} + r_{i+2}$ $(\nu(r_{i+2}) < \nu(r_{i+1}))$

On pose $u_{i+2} = u_i - q_{i+2} u_{i+1}$, $v_{i+2} = v_i - q_{i+2} v_{i+1}$
Alors il existe un rang $n_0$ tel que $r_{n_0} \neq 0$ et on a
$a u_{n_0} + b v_{n_0} = a \wedge b = r_{n_0}$ $(\forall n \geq n_0+1,\ r_n = 0)$

**Rq 26 :** Cet algorithme étendu sert à obtenir le Bézout

**Ex 27** Donc $\mathbb{Z}$, on a $114 \wedge 76 = 38$
En effet $w_0 = \begin{bmatrix} 114 \\ 1 \\ 0 \end{bmatrix}$, $w_1 = \begin{bmatrix} 76 \\ 0 \\ 1 \end{bmatrix}$

- $114 = 1 \times 76 + \underbrace{38}_{\text{Dernier reste non nul}} \Rightarrow r_2 = 38,\ q_2 = 1$
  $u_2 = 1 - 1 \times 0 = 1$
  $v_2 = 0 - 1 \times 1 = -1$
  $w_2 = \begin{bmatrix} 38 \\ 1 \\ -1 \end{bmatrix}$
- $76 = 2 \times 38 + 0$

Donc $114 \wedge 76 = 38$

**Rq 28 :** Le nombre d'itérations est le même, mais le nombre d'appels à chaque étape est en revanche différent

## III - Applications

### 1 - Arithmétique dans $\mathbb{Z}$

**Prop 29** (Equation diophantienne) L'équation diophantienne $ax + by = c$ d'inconnue $(x, y) \in \mathbb{Z}^2$ admet des solutions si et seulement si $a \wedge b \mid c$. L'ensemble des solutions est donné par $\left\{ \left(\frac{b}{a \wedge b} k + x_0, -\frac{a}{a \wedge b} k + y_0\right),\ k \in \mathbb{Z} \right\}$ où $(x_0, y_0)$ est une solution particulière (« évidente »), où $a = \frac{a}{a \wedge b}$, $b = \frac{b}{a \wedge b}$

**Ex 30 :** L'équation $114x + 76y = 38$ a pour ensemble de solutions l'ensemble $\left\{ (2k + 1, -3k - 1),\ k \in \mathbb{Z} \right\}$

**Prop 31** (Lemme chinois pour les entiers relatifs)
Si $m \wedge n = 1$, alors $\frac{\mathbb{Z}}{mn\mathbb{Z}} \xrightarrow{\sim} \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$ est un isomorphisme de groupes ($\mathbb{Z}^*$ de la classe de $x$ modulo $n$)
$[x]_{mn} \longmapsto ([x]_m, [x]_n)$

**Appli 32** (Système de congruences) Soient $m_1, \dots, m_n \in \mathbb{N}^*$ des entiers premiers entre eux. Soient $a_1, \dots, a_n \in \mathbb{N}$. Alors le système de congruences
$\begin{cases} x \equiv a_1 \ [m_1] \\ \vdots \\ x \equiv a_n \ [m_n] \end{cases}$ d'inconnue $x \in \mathbb{Z}$ admet pour solutions $\{x_0 + m_1 \dots m_n k,\ k \in \mathbb{Z}\}$ où $x_0$ est une solution particulière de ce système

**Ex 33 :** Le système $\begin{cases} x \equiv 2 \ [5] \\ x \equiv 5 \ [7] \end{cases}$ admet pour solution l'ensemble $\{-12 + 35k,\ k \in \mathbb{Z}\}$

**Prop 34 :** Soient $n, p \in \mathbb{Z}$. $[n]$ admet une inverse dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ si et seulement si $n \wedge p = 1$

Prop 35 : $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps $\Leftrightarrow$ $p$ est premier on le note $\mathbb{F}_p$

Th 36 (Triplets Pythagoriciens) :
Les $(x,y,z) \in \mathbb{Z}^3$ qui vérifient $x^2+y^2=z^2$ sont exactement ceux de la forme $(a(q^2-p^2), 2apq, a(p^2+q^2))$ avec $a \in \mathbb{Z}$ et $p,q \in \mathbb{Z}$ de entiers premiers entre eux

DVPT 1

Ex 37

(i) $3^2 = 3^2 + 4^2$
(ii) $13^2 = 12^2 + 5^2$

(cf. Fig 1)

## 2 - Arithmétique dans $\mathbb{K}[X]$

Prop 38 : Soit $P, Q \in \mathbb{K}[X]$ $P$ est inversible dans $\frac{\mathbb{K}[X]}{\langle Q \rangle}$ si, et seulement si $P \wedge Q = 1$

Prop 39 : $\frac{\mathbb{K}[X]}{\langle Q \rangle}$ est un corps ssi $Q$ est irréductible dans $\mathbb{K}[X]$

Application : Construction de corps finis à $p^m$ éléments

Ex 40 : $\frac{\mathbb{F}_2[X]}{\langle X^2+X+1 \rangle}$ est un corps à 4 éléments

Prop 41 : Si $\mathrm{Car}(\mathbb{K}) = 0$, $P$ et $P'$ sont premiers entre eux $\Leftrightarrow P \wedge P' = 1$

Th 43 (Algorithme de Berlekamp)
Soit $P \in \mathbb{F}_q[X]$ dont la décomposition en polynômes irréductibles est $P = \prod_{i=1}^{r} P_i$ avec $P_i = X^p - X \in \frac{\mathbb{F}_q[X]}{\langle P \rangle}$. L'algorithme suivant détermine au bout d'un nombre fini d'étapes et donne la décomposition en irréductibles de $P$ :
1 - On calcule la matrice de $S_p : \frac{\mathbb{F}_q[X]}{\langle P \rangle} \to \frac{\mathbb{F}_q[X]}{\langle P \rangle}$, $Q \mapsto Q^q$ dans la base $\{1, X, \dots, X^{\deg(P)-1}\}$
2 - Le nombre de facteurs irréductibles de $P$ est $r = \dim(\ker(S_p - Id)) = \deg(P) - \mathrm{rg}(S_p - Id)$. Si $r=1$, on arrête, $P$ est irréductible. Sinon, on va en [3]
3 - On calcule $V \in \mathbb{F}_q[X] \setminus \overline{V}^P \neq$ Polynôme constant de $\mathbb{F}_q[X]$, $V \in \ker(S_p - Id)$
On a $P = \prod_{a \in \mathbb{F}_q} \mathrm{PGCD}(P, V - ca)$, calculé avec l'algorithme d'Euclide. On applique [2] aux facteurs

DVPT 2

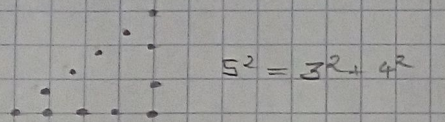
## 3 - En algèbre linéaire

Th 44 (Lemme des noyaux) : Soient $P_1, \dots, P_m \in \mathbb{K}[X]$, deux à deux premiers entre eux, soit $E$ un $\mathbb{K}$-espace vectoriel et $u \in \mathrm{End}_{\mathbb{K}}(E)$ tels que
$$\ker(P_1 \cdots P_m)(u) = \bigoplus_{i=1}^{m} \ker(P_i(u))$$

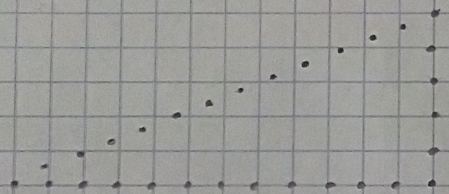
Appl 45 : Si $u \in \mathrm{End}_{\mathbb{K}}(E)$, $E$ est un $\mathbb{K}$-espace vectoriel de dim finie, alors $\chi_u = \prod_{\lambda \in \mathrm{Sp}_{\mathbb{K}}(u)} (X-\lambda)^{m_\lambda}$ est le polynôme caractéristique de $u$
On a : $E = \bigoplus_{i=1}^{d} \ker\left[(u - \lambda_i \mathrm{Id}_E)^{m_i}\right]$

Th 46 (Forme normale de Smith) : Si $A$ est euclidien
Soit $M \in \mathcal{M}_{n,m}(A)$ Alors $\exists P \in GL_n(A)$, $\exists Q \in GL_m(A)$ telles que :
$$PMQ = \begin{bmatrix} d_1 & (0) & \\ & \ddots & \\ (0) & & d_r \\ & & (0) \end{bmatrix}$$
où $d_i \in A$ et $\forall i \in [\![1, r-1]\!]$, $d_i \mid d_{i+1}$

Annexe :



$5^2 = 3^2 + 4^2$



$13^2 = 5^2 + 12^2$

Deux exemples de triplets pythagoriciens Fig 1


Références

D. Perrin, Cours d'algèbre

J. Calais, Éléments de théorie des anneaux