142 — PGCD et PPCM, algorithmes de calcul. Applications.

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

Dans cette section, A est un anneau intègre (commutatif) et $(a,b,a_1,\dots,a_r)\in A^{r+2}$

A- Première définition, existence, cas des anneaux factoriels

Def 1: Si $a_1 \cdots a_r \neq 0$, alors sous réserve d'existence, on appelle PGCD (resp. PPCM) de $a_1,\dots,a_r$, noté $a_1\wedge\cdots\wedge a_r$ ou $\mathrm{pgcd}(a_1,\dots,a_r)$ (resp. $a_1\vee\cdots\vee a_r$ ou $\mathrm{ppcm}(a_1,\dots,a_r)$) un plus grand minorant (resp. un plus grand majorant) de $\{a_1,\dots,a_r\}$ pour la relation (binaire) de divisibilité. On pose par ailleurs $0\wedge 0 = 0 \vee a = 0$.

En particulier, le PGCD et le PPCM sont associatifs et commutatifs : $a\wedge b = b\wedge a$, $a_1\wedge a_2\wedge a_3\wedge a_4\wedge a_5 = (a_1\wedge a_2)\wedge(a_3\wedge a_4)\wedge a_5$.

Rq 2: Les PGCD (resp. PPCM) de $a_1,\dots,a_r$ sont tous associés. L'écriture $d = a_1\wedge\cdots\wedge a_r$ est un abus signifiant "d est un PGCD de $a_1,\dots,a_r$".

[R] 246 **Prop 3**: Si a et b ont un PPCM alors ils ont un PGCD $a\wedge b = ab\,(a\vee b)^{-1}$.

Ex 4: 3 et $2+i\sqrt{5}$ ont un PGCD mais pas de PPCM dans $\mathbb{Z}[i\sqrt{5}]$.

4 et $2+2i\sqrt{3}$ n'ont pas de PGCD dans $\mathbb{Z}[i\sqrt{3}]$.

Def 5: On dit que $a_1,\dots,a_r$ sont premiers entre eux (dans leur ensemble) si $a_1\wedge\cdots\wedge a_r = 1$. On dit $a_1,\dots,a_r$ sont deux à deux premiers entre eux si $\forall (i,j)\in [\![1,r]\!]^2,\ i\neq j \Rightarrow a_i\wedge a_j = 1$.

[R] 247 **Thm 6** (de Gauss) : $\forall (a,b,c)\in A^3$, $\begin{cases} a\mid bc \\ a\wedge b = 1\end{cases} \Rightarrow a\mid c$.

[R] 246 **Prop 7**: Si toute paire d'éléments de A admet un PGCD (on dit alors que A est un anneau à PGCD), alors toute paire d'éléments de A admet un PPCM, et la réciproque est vraie.

[P] 49 **Prop 8** : Supposons A factoriel, notons $\mathcal{P}$ un système complet de représentants des irréductibles de A.

$$\prod_{p\in\mathcal{P}} p^{\min(v_p(a),\,v_p(b))} \text{ est un PGCD de } a \text{ et } b.$$

$$\prod_{p\in\mathcal{P}} p^{\max(v_p(a),\,v_p(b))} \text{ est un PPCM de } a \text{ et } b.$$

Def 9 : Si $A=\mathbb{Z}$ (resp. $A=K[X]$, K un corps), alors le PGCD de a et b est l'unique PGCD de a et b qui est positif (resp. unitaire).

B- Situation dans les anneaux principaux

On suppose A principal.

Prop 10: $m\in A$ est un PPCM de a et b si, et seulement si $aA\cap bA = mA$.

$d\in A$ est un PGCD de a et b, si, et seulement si $aA+bA = dA$.

Thm 11 (de Bézout) : $(\exists (u,v)\in A^2 : au+bv=1) \Leftrightarrow a\wedge b = 1$

Rq 12: $\forall (a,b)\in A^2$, $\exists (u,v)\in A^2 : au+bv = a\wedge b$. Le théorème de Bézout indique que réciproque est vraie si $a\wedge b = 1$ (Cex : $3\times(2)+2\times(-2) = 2$, mais $3\wedge 2\neq 2$). [R] 247

Def 13: Un couple $(u,v)\in A^2$ tel que $a\wedge b = au+bv$ est appelé couple de Bézout de (a,b), et l'égalité est appelée relation de Bézout.

Appli 14 : Résolution de $ax+by=c$ $(a\wedge b = 1)$.

Appli 15: Lemme des noyaux : soit $(P,Q)\in K[X]^2$ tel que $P\wedge Q = 1$. Soient V un K-espace vectoriel de dimension finie. Pour tout endomorphisme f de V, $\mathrm{Ker}((PQ)(f)) = \mathrm{Ker}(P(f)) \oplus \mathrm{Ker}(Q(f))$.

Thm 16 (des restes chinois) : Si $a_1,\dots,a_r$ sont non nuls, non inversibles et deux à deux premiers entre eux, alors : **DEV 1** [R] 250

$$\varphi : x \bmod a_1\cdots a_r \longmapsto (x \bmod a_1, \dots, x \bmod a_r)$$

est un isomorphisme d'anneaux de $A/\langle a_1\cdots a_r\rangle$ dans $A/\langle a_1\rangle \times\cdots\times A/\langle a_r\rangle$

Posons $a = a_1\cdots a_r$ et pour $j\in[\![1,r]\!]$, $b_j = \frac{a}{a_j}$. Il existe $(u_1,\dots,u_r)\in A^r$ telle que $\sum_{i=1}^{r} u_i b_i = 1$. La réciproque de φ s'exprime alors :

$$\varphi^{-1} : (x_1 \bmod a_1, \dots, x_r \bmod a_r) \longmapsto \sum_{i=1}^{r} x_i u_i b_i \bmod a_1\cdots a_r$$

Appli 17 : Résolution d'un système de congruence. [R] 251

Ex 18 : Interpolation de Lagrange : soient $x_1,\dots,x_n\in K$ deux à deux distincts et $(y_1,\dots,y_n)\in K^n$. Un polynôme interpolateur des x_i en y_i est une solution du système $\{\forall i\in[\![1,n]\!],\ P \equiv y_i\ [X-x_i]$.

Ex 19 : Recherche de $P \in \mathbb{Z}/5\mathbb{Z}[X]$ tel que $P(\bar{0})=\bar{2}$, $P(\bar{1})=\bar{0}$, $P(\bar{2})=\bar{1}$ de degré minimal. **DEV 1**

[R] 298 **Prop 20** : $\forall (n,m) \in \mathbb{N}_{\geq 2}^2$, $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/n\wedge m\mathbb{Z} \times \mathbb{Z}/n\vee m\mathbb{Z}$.

II - Algorithmes de calcul dans un anneau euclidien

Dans cette section, A est supposé euclidien. Soit $(a,b) \in A \times A\setminus\{0\}$.

A - Algorithmes d'Euclide

[R] 264 **Lemme 21** (d'Euclide) : Si $a=bq+r$ avec $(q,r)\in A^2$, alors $a\wedge b = b\wedge r$.

[R] 264 **Algo 22** (d'Euclide) : Posons $r_{-1}=a$ et $r_0=b$, et pour $n\geq 1$, r_n est un reste d'une division euclidienne de r_{n-2} par r_{n-1} si $r_{n-1}\neq 0$, et $r_n=0$ sinon. Il existe $N\in\mathbb{N}$ tel que $\forall n \geq N+1$, $r_n=0$; de plus, $a\wedge b = r_N$.

Ex 23 : $M_n \wedge M_m = M_{n\wedge m}$ où $(n,m)\in\mathbb{N}^2$ et $M_n = 2^n-1$.

$(X^n-1)\wedge(X^m-1) = X^{m\wedge n}-1$.

[R] 265 **Algo 24** (d'Euclide étendu) : Soit $(q_n)_{n\geq 1}$ une suite de quotients dans l'algorithme d'Euclide, soit N le rang du dernier reste non nul. On peut trouver un couple de Bézout en "remontant" l'algorithme d'Euclide, i.e. en écrivant $a\wedge b = r_N = r_{N-2} - q_N r_{N-1}$, puis en y substituant $r_{N-1} = r_{N-3} - q_{N-1} r_{N-2}$, puis en y substituant $r_{N-2} = r_{N-4} - q_{N-2} r_{N-3}$, etc. jusqu'à exprimer $a\wedge b$ sous la forme $a\wedge b = a\, f(q_1,\dots,q_N) + b\, g(q_1,\dots,q_N)$.

Appli 25 : Calcul d'un inverse dans un corps de rupture : soit $K = \mathbb{Q}[X]/\langle X^2-X-1\rangle \simeq \mathbb{Q}(\varphi)$. Dans K, $(2\varphi+1)^{-1} = 2\varphi - 3$.

Prop 26 : $GL_2(\mathbb{Z})$ agit sur $\mathbb{Z}^2$ par $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\cdot\begin{pmatrix}a\\ b\end{pmatrix} = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}a\\ b\end{pmatrix} = \begin{pmatrix}\alpha a+\beta b\\ \gamma a+\delta b\end{pmatrix}$.
Les orbites de cette action sont les $E_d = \{\begin{pmatrix}a\\ b\end{pmatrix}\in\mathbb{Z}^2 \mid a\wedge b = d\}$, $d\in\mathbb{N}$.

Cor 27 : D'après l'algorithme d'Euclide, $\forall (a,b)\in\mathbb{Z}^2\ \exists P\in GL_2(\mathbb{Z}) : P\begin{pmatrix}a\\ b\end{pmatrix} = \begin{pmatrix}a\wedge b\\ 0\end{pmatrix}$

Appli 28 : Soit $a=(a_1,\dots,a_n)$ un vecteur de $\mathbb{Z}^n$. On peut compléter (a) en une $\mathbb{Z}$-base de $\mathbb{Z}^n$ si, et seulement si $a_1\wedge\dots\wedge a_n \sim 1$.

B - Du côté de $\mathbb{Z}$ et $K[X]$, un point sur la complexité

Dans le cas de la division euclidienne dans $\mathbb{Z}$, on impose aux restes d'être positifs, ce qui rend les reste et quotient uniques.

Thm 29 (de Lamé) : Supposons que $a>b\geq 1$. Soient $(F_k)_k$ la suite de Fibonacci [D] 38
débutant à 0, et $k\in\mathbb{N}$ tel que $b<F_{k+1}$. L'algorithme d'Euclide pour a et b termine en moins de k étapes.

Rq 30 : Cette majoration est optimale : considérer $a=F_{k+1}$, $b=F_k$.

Algo 31 (PGCD binaire) : Supposons $a\geq b\geq 0$. La fonction : [D] 36

```
Fonction PGCD_binaire(a,b) :
    Si a = 0 : renvoyer b
    Si 2|a et 2|b : renvoyer 2 x PGCD_binaire(a/2, b/2)
    Si 2|a et non(2|b) : renvoyer PGCD_binaire(a/2, b)
    Si non(2|a) et 2|b : renvoyer PGCD_binaire(a, b/2)
    Sinon : renvoyer PGCD_binaire((a-b)/2, b)
```

appliquée à (a,b) renvoie $a\wedge b$.

Rq 32 : Algo 31 se termine en au plus $\lceil \log_2(a)\rceil$ récursions.

Prop 33 : Soit $(P,Q)\in K[X]^2$ tel que $n := \deg(P) \geq \deg(Q) \geq 1$. L'algorithme d'Euclide appliqué à P et Q termine en au plus n étapes.

III - Applications en arithmétique et en théorie des groupes

A - (Systèmes d') équations diophantiennes linéaires

Def 34 : Soit $M\in M_{n,m}(\mathbb{Z})$. On dit que M est sous forme normale d'Hermite [G] 163
si elle est sous la forme :

$$\begin{pmatrix}
0\cdots 0 & p_1 & *\cdots* & + & *\cdots* & + & & & \\
 & & & p_2 & *\cdots* & + & & & \\
 & & & & & p_3 & \cdots & & \\
 & & & & & & \cdots & + & *\cdots* \\
 & & & & & & & p_r & *\cdots* \\
 & & & & & & & & 0 \\
 & & & & & & & & \vdots \\
 & & & & & & & & 0
\end{pmatrix}$$

où les pivots p_i sont strictement positifs, et les coefficient au dessus de chaque pivot sont positifs et inférieurs au pivot.

[G] 164 <u>Algo 35</u> (d'Hermite) : Soit $M\in\mathcal{M}_{n,m}(\mathbb{Z})\setminus\{0\}$.

On définit $\delta_{i_0,j}(M)=\min\{|M_{i,j}| : i\geq i_0, M_{i,j}\neq 0\}$ et $\delta_{i_0,j}(M)=0$ si l'ensemble est vide. L'algorithme d'Hermite :

> Soit $i_0=1$. Tant que $i_0<n$: soit $j_0=\min\{1\leq j\leq m \mid \delta_{i_0,j}(M)\neq 0\}$
> - Si $\forall i>i_0$, $M_{i,j_0}=0$, alors $L_{i_0}\leftarrow \mathrm{sg}(M_{i_0,j_0})L_{i_0}$, et pour i allant de 1 à i_0-1, $L_i\longleftarrow L_i-q_iL_{i_0}$ où q_i est le quotient de la division euclidienne de M_{i,j_0} par M_{i_0,j_0}.
>   On remplace i_0 par i_0+1.
> - Sinon, soit $k\in[\![i_0,n]\!]$ tel que $|M_{k,j_0}|$ soit non nul et minimal. On effectue $L_i\Leftrightarrow L_{i_0}$ puis, pour i allant de i_0+1 à n, $L_i\leftarrow L_i-q_iL_{i_0}$

transforme M sous une forme normale d'Hermite M_H. En particulier, il existe $P\in GL_n(\mathbb{Z})$ telle que $M_H=PM$.

<u>Appli 36</u> : Résolution d'un système d'équations diophantiennes linéaires.

<u>Ex 37</u> : Cas d'une seule équation linéaire (E) : ${}^t\begin{pmatrix}a_1\\ \vdots\\ a_n\end{pmatrix}\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=b$, avec $a_1\wedge\cdots\wedge a_n=1$. D'après Cor 24, il existe $P\in GL_n(\mathbb{Z})$ telle que ${}^t\begin{pmatrix}a_1\\ \vdots\\ a_n\end{pmatrix}P={}^t\begin{pmatrix}a_1\wedge\cdots\wedge a_n\\ 0\\ \vdots\\ 0\end{pmatrix}={}^t\begin{pmatrix}1\\ 0\\ \vdots\\ 0\end{pmatrix}$. De là, (E) $\Leftrightarrow {}^t\begin{pmatrix}1\\ 0\\ \vdots\\ 0\end{pmatrix}\begin{pmatrix}\tilde{x}_1\\ \vdots\\ \tilde{x}_n\end{pmatrix}=b \Leftrightarrow \tilde{x}_1=b$ où $\begin{pmatrix}\tilde{x}_1\\ \vdots\\ \tilde{x}_n\end{pmatrix}=P^{-1}\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$. Donc $S(E)=\left\{P\begin{pmatrix}1\\ x_2\\ \vdots\\ x_n\end{pmatrix} : (x_2,\dots,x_n)\in\mathbb{Z}^{n-1}\right\}$.

B- Un théorème de Liouville

<u>Thm 38</u> (Liouville) : L'équation $P^n+Q^n+R^n=0$ n'admet pas de solution non triviale (i.e. P,Q,R non associés) dans $\mathbb{C}[X]$ dès lors que $n\geq 3$. **DEV 2** [FGN] 179 [R] 404

C- Quelques résultats en théorie des groupes

Soit G un groupe fini. On note $\mathrm{ord}(g)$ l'ordre de $g\in G$ dans G.

<u>Prop 39</u> : L'exposant de G ($\max\limits_{g\in G}\mathrm{ord}(g)$) vaut $\mathrm{ppcm}(\{\mathrm{ord}(g)\}_{g\in G})$. [R] 9

<u>Lemme 40</u> : Soit $n\in\mathbb{N}\setminus\{0,1\}$, soit $\bar{d}\in\mathbb{Z}/n\mathbb{Z}$. On a $\mathrm{ord}(\bar{d})=\dfrac{n}{n\wedge d}$. [R] 28

<u>Thm 41</u> (de structure des groupes abéliens finis). [R] 28

Supposons G abélien, de cardinal au moins 2. Il existe $(d_1,d_2,\dots,d_s)\in(\mathbb{N}\setminus\{0,1\})^s$ tels que :

$$G\simeq \mathbb{Z}/d_1\mathbb{Z}\times\cdots\times\mathbb{Z}/d_s\mathbb{Z}\quad,\quad d_1\mid d_2\mid\cdots\mid d_s$$

Les entiers $d_1,\dots,d_s$, appelés facteurs invariants de G, sont uniques et déterminent la classe d'isomorphisme de G.

<u>Ex 42</u> : Soit p un nombre premier. Un groupe abélien d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$.

<u>Références</u> :

[FGN] : Exercices de mathématiques – Oraux X-ENS – Algèbre 1. (Serge Francinou, Hervé Gianella, Serge Nicolas)

[D] : Cours d'algèbre (Michel Demazure)

[R] : Mathématiques pour l'agrégation – Algèbre et géométrie (2e édition) (Jean-Étienne Rombaldi)

[P] : Cours d'algèbre (Daniel Perrin)

[G] : Algèbre I – Groupes, corps et théorie de Galois (Daniel Guin, Thomas Hausberger)