Leçon 142 : PGCD et PPCM. Algorithmes de calculs. Applications.

CLERC Gauthier
CHAUDY Lucie
ESLOT Coralie

Dans la suite, $\mathbb{K}$ est un corps commutatif, et A un anneau non trivial, commutatif et unitaire, d'unité 1.

I) Cadre et définitions

1) Divisibilité

Def 1: On appelle ensemble des inversibles de A
$$A^* = \{a \in A \mid \exists b \in A \text{ tq } ab = 1\}.$$

Ex 2: $\mathbb{K}^* = \mathbb{K} - \{0\}$; $\mathbb{K}[X]^* = \mathbb{K}^*$; $\mathbb{Z}^* = \{\pm 1\}$

Def 3: On dit que $a \mid b$ si $\exists c \in A$ tq $b = ac$

Ex 4: Soit $a, b \in \mathbb{R}$; $a + bi \mid a^2 + b^2$ dans $\mathbb{C}$

Def/prop 5: On associe à la divisibilité une relation d'équivalence : $a \sim b \iff a \mid b$ et $b \mid a$

A est désormais supposé intègre

Ex 6: Soit $z \in \mathbb{Z}$, alors $z \sim -z$

Prop 7: $a \sim b \iff \exists v \in A^*$ tq $v = ab$

Remarque 8: la divisibilité n'est donc pas une relation d'ordre puisque pas antisymétrique en générale, pour obtenir l'antisymétrie il faut "se débarasser des inversibles".

Prop 9:
$$A/\sim \;\longrightarrow I(A) = \{\text{idéaux principaux de } A\}$$
$$\bar{a} \longmapsto (a)$$
est un isomorphisme d'ensemble ordonné où $A/\sim$ est munit de l'ordre induit par la divisibilité et $I(A)$ de l'inclusion inverse.

Def 10: Soit $p \in A$. On dit que p est irréductible ssi : $p \notin A^*$ et $(p = ab \Rightarrow a$ ou $b \in A^*)$

Ex 11:
- $\{0\}$ n'est pas irréductible
- X^2+1 est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

Def 12: Soit $a, b \in A$, a et b sont dit premiers entre eux si $(d \mid b$ et $d \mid a \Rightarrow d \in A^*)$

2) Anneaux factoriels

On notera $\mathcal{P}$ un ensemble de représentants de $\{a \in A \mid a \text{ irréductible}\}/\sim$

Ex 13: Dans $\mathbb{Z}$ on prend pour $\mathcal{P}$ l'ensemble des nombres premiers positifs.

Def 14: A est dit factoriel si tout éléments de A s'écrit de manière unique sous la forme
$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$$
ou $u \in A^*$ et un nombre fini de v_p non nuls

Remarque 15: Soit $a, b \neq 0$ des éléments d'un anneau factoriel alors : $a \mid b \iff \forall p \in \mathcal{P}\ v_p(a) \leq v_p(b)$

Théorème 16: Soit A un anneau factoriel, $p \in \mathcal{P}$, $a, b, c \in A$ alors :
- Euclide : $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$
- Gauss : Si $a \mid bc$ et a et b sont premiers alors $a \mid c$

Def 17: A est dit principal si tous ses idéaux sont principaux.

Thm 18: Un anneau principal est factoriel.

3) PPCM et PGCD

Prop/Def 19: Si A est factoriel alors $A/\sim$ est un treillis. Alors si $\inf((a),(b)) = (c)$ et $\sup((a),(b)) = (d)$ on pose $d = \mathrm{pgcd}(a,b)$ et $c = \mathrm{ppcm}(a,b)$

Remarque 20:
- Il s'agit bien du sup et de l'inf pour l'inclusion.
- PPCM et PGCD sont donc définis aux inversibles près, on choisira un représentant commode au cas par cas.
- Si $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ et $b = v \prod_{p \in \mathcal{P}} p^{v_p(b)}$ alors
$$\mathrm{pgcd}(a,b) = \{z \prod_{p \in \mathcal{P}} p^{\inf(v_p(a), v_p(b))} \mid z \in A^*\}.$$

Proposition 21: Dans un anneau principal, $a, b \in A - \{0\}$ et $d = \mathrm{pgcd}(a,b)$ alors $(d) = (a) + (b)$.

Exc 22 : • $\mathbb{K}[X,Y]$ est factoriel mais non-principal ; X et Y sont premiers entre eux mais $(X)+(Y)\neq(1)$.

• $A=\{a+ib\sqrt{5} \mid a,b\in\mathbb{Z}\}\subseteq\mathbb{C}$ donc intègre mais en posant $p=2+i\sqrt{5}$, $q=\bar{p}$, $a=pq$ et $b=3p$; a et b n'ont pas de pgcd.

4) Anneaux euclidiens

Déf 23 : $(A;N)$ est euclidien si :
1) A est intègre 2) $N: A-\{0\}\to\mathbb{N}$ tq si $a,b\neq0$ $\exists q,r\in A$ tels que $a=bq+r$ et ($r=0$ ou $N(r)<N(b)$)

Théorème 24 : Un anneau euclidien est principal.

Théorème 25 : Soit $P\in A[X]$; $P\neq0$ de coeff dominants inversibles alors : $\forall F\in A[X]$; $\exists Q,R\in A[X]$ tels que $F=PQ+R$ et ($d^\circ R<d^\circ P$ ou $R=0$)

Exemples 26 : • $(\mathbb{K}[X];d^\circ)$ est euclidien.
• $(\mathbb{Z}[i];N)$ où $\forall z\in\mathbb{Z}[i]$ $N(z)=z\bar{z}$ est euclidien, d'inversibles $(\mathbb{Z}[i])^*=\{\pm1;\pm i\}$ appelé anneau des entiers de Gauss.
• $(\mathbb{Z};|\cdot|)$ est euclidien.

II Calculs par les algorithmes

Théorème 27 : On dispose d'algorithmes pour calculer effectivement des divisions euclidiennes dans $\mathbb{Z}$ et dans $A[X]$, sous les hypothèses du thm 25.

Exemple 28 : • $\mathrm{div}(18,7)\to(0,18,7)\to(1,11,7)\to(2;4;7)$
• Dans $\mathbb{Z}[X]$: $\mathrm{div}(3X^2+5X+2 ; X+3)\to(0;3X^2+5X+2;X+3)\to\dots\to(3X-4;14;X+3)$
• Dans $\mathbb{F}_3[X]$: $\mathrm{div}(X^3+2X^2+2X+1;X^2+2)\to(0;X^3+2X^2+2X+1;X^2+2)\to(X;2X^2+1;X^2+2)\to(X+2;0;X^2+2)$

Notation 29 : Dans un anneau euclidien on notera $(a\div b)$ le quotient dans la division euclidienne de a par b.

Algo 30 : (Euclide)
Entrées : u,v et euclidien
Règles : $[u\neq0]$: $(u,v)\mapsto(v-(v\div u)u;u)$
$[u=0]$ $(u,v)\mapsto v$

Théorème 31 : L'algorithme précédent termine et retourne le pgcd des deux éléments d'entrée.

Déf 32 : On définit la suite de Fibonacci par $F_0=0$, $F_1=1$ et $F_{n+1}=F_{n-1}+F_n$.

Prop 33 : Soit $x,y\in\mathbb{N}$; $x\geq y$ de pgcd (d). Si l'algo d'Euclide usuel s'arrête au bout de n pas alors :
$$x\geq dF_{n+2} \text{ et } y\geq dF_{n+1}$$

Cor 34 : Soit $x,y\in\mathbb{N}$ avec $0\leq x\leq y$, l'algo d'Euclide prend au plus $\frac{3}{2}\log y+1$ pas pour calculer leur pgcd.

III Applications

1) Factorisation des polynômes sur les corps finis

Thm 35 : Soit $\mathbb{K}$ un corps fini de car $p>0$ à q éléments. a) $\mathbb{K}$ est un $\mathbb{F}_p$-ev de dim r finie, et $q=p^r$
b) $\mathbb{K}^*$ est cyclique d'ordre $q-1$
c) Tout élément x de $\mathbb{K}$ vérifie $x^q=x$

Lemme 36 : Soit p un nombre premier, $s\in\mathbb{N}$ et $q=p^s$, $R\in\mathbb{F}_q[X]$ alors :
$$S_R:\mathbb{F}_q[X]/(R)\to\mathbb{F}_q[X]/(R)$$
$$(Q(X) \bmod R)\mapsto Q(X^q) \bmod R$$

est linéaire et coïncide avec l'élévation à la puissance q dans $\mathbb{F}_q[X]/(P)$.

Lemme 37 : (Isomorphisme chinois)
Soit $\mathbb{K}$ un corps commutatif et $P_1;\dots;P_r \in \mathbb{K}[X]$ deux à deux premiers entre eux, alors on dispose de l'isomorphisme :

$$\mathbb{K}[X]/(P_1\dots P_r) \longleftrightarrow \mathbb{K}[X]/(P_1) \times \dots \times \mathbb{K}[X]/(P_r)$$
$$Q \bmod P_1\dots P_r \longmapsto (Q \bmod P_1;\dots;Q \bmod P_r)$$

Dev 1

Algorithme 38 : Soit q une puissance d'un nombre premier. On dispose d'un algorithme effectif pour factoriser tous les polynômes de $\mathbb{F}_q[X]$ sans facteurs carrés en produit d'irréductibles.

Remarque 39 : On peut se ramener au cas où P n'a pas de facteur carré en calculant $\operatorname{pgcd}(P,P')$. Grâce au lemme suivant :

Lemme 40 : Dans un corps $\mathbb{K}$, soit $P \in \mathbb{K}[X]$; alors $\operatorname{pgcd}(P,P') = 1 \Leftrightarrow P$ est sans facteurs carrés.

2) Un exemple d'équation diophantienne : Sophie-Germain

Déf 41 : Un nombre premier p est dit nombre de Sophie-Germain si $q = 2p+1$ est un nombre premier.

Ex 42 : $2, 3, 5, 11, 23$ et $1093307 \cdot 2^{66452} - 1$ sont des nombres de Sophie-Germain.

Dev 2

Thm 43 : Soit p un nombre de Sophie-Germain alors :
$$\nexists (x,y,z) \in \mathbb{Z}^3 \text{ tq } xyz \not\equiv 0 \bmod p$$
$$\text{et } x^p + y^p + z^p = 0$$

3) Matrices à coefficients dans les anneaux principaux

Soit (A,N) un anneau principal

Def 44 : On appelle matrices élémentaires d'ordre n les matrices de l'une des formes suivantes :
- les matrices de transposition : pour $\sigma \in S_n$; P_σ a pour coefficients $p_{ij} = \delta^{j}_{\sigma(i)}$
- les matrices $I_n + aJ_{ik}$ pour $a \in A$ et $1 \le i \ne k \le n$ avec $(J_{ik})_{lm} = \delta^l_i \delta^m_k$
- les matrices diagonales inversibles

Thm 45 : Pour A euclidien, $GL_n(A)$ est l'ensemble des matrices qui sont produit de matrices élémentaires

Thm 46 : A principal. $\exists P \in GL_n(A)$; $Q \in GL_m(A)$ et $D \in \mathcal{M}_{n\times m}(A)$ quasi-diagonale tq
- $M = PDQ$
- $d_1 | d_2 ; \dots ; d_i | d_{i+1} ; \dots$

Cette décomposition est unique aux inversibles près.

Cor 47 : Dans le cadre euclidien, M est donc élémentairement équivalente à une telle matrice D. On note $M \underset{E}{\sim} M'$ si M et M' sont élémentairement équivalentes.

Ex 48 : $\begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix} \underset{E}{\sim} \begin{pmatrix} 0 & 1 \\ -7 & 5 \end{pmatrix} \underset{E}{\sim} \begin{pmatrix} 1 & 0 \\ 5 & 7 \end{pmatrix} \underset{E}{\sim} \begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix}$

Application 49 : (Structure de GAF)
Soit G un GAF, $\exists ! n \in \mathbb{N}$ et une unique suite d'entiers naturels $d_n \ge d_{n-1} \ge \dots \ge d_1 > 1$ tq $d_i | d_{i+1}$ et
$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_n\mathbb{Z}$$

Ex 50 : $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

Références : D. Perrin - Cours d'algèbre
M. Demazure - Cours d'algèbre
FGN : Algèbre I
D. Serre - Matrices
Beck, Malick-Peyré - Objectif agrégation
J.P. Escoffier - Théorie de Galois

Division euclidienne dans $\mathbb{Z}$ ①

Entrées : entiers a et b avec $b>0$
Sorties : b inchangé, entier q, r avec $a = bq + r$ et $0 \leq r < b$
Règles :
$\mathrm{div}(a,b) \longmapsto (0,a,b)$
$[r<0] : (q,r,b) \longmapsto (q-1; r+b; b)$
$[r \geq b] : (q,r,b) \longmapsto (q+1; r-b; b)$
$[0 \leq r < b]$: retourner (q,r,b)

Division euclidienne des polynômes ②

Entrées : Polynômes U et V avec $\mathrm{dom}(V)$ inversible
Sorties : Polynômes Q et R avec $U = VQ + R$ et $d^\circ R < d^\circ V$
Règles :
$(U,V) \longmapsto (0,U,V)$
$[\deg(R) \geq \deg(V)] : (Q,R,V) \longmapsto (Q+A; R-AV; V)$
où $A = \dfrac{\mathrm{dom} R}{\mathrm{dom}(V)} X^{\deg(R)-\deg(V)}$

$[\deg(R) < \deg(V)] : (Q,R,V) \longmapsto (Q,R)$

Algorithme d'Euclide ③

Entrées : x, y deux éléments d'un anneau euclidien
Sorties : $\mathrm{pgcd}(x,y)$
Règles : $[x \neq 0] : (x,y) \longmapsto (y - (y \div x)x; x)$
$[x = 0] : (x,y) \longmapsto y$

Berlekamp ①

Entrées : q le cardinal du corps ; $P \in \mathbb{F}_q[X]$ sans facteurs carrés,
$\sigma : \mathbb{F}_q \to [\![1;q]\!]$ bijective

ⓘ Calcul de la matrice de $S_p - Id$ en effectuant les divisions euclidiennes de X^{jq} par P pour $0 \leq j \leq \deg(P)-1$

ⓘⓘ Calcul d'une base de $\mathrm{Ker}(S_p - Id)$ grâce à l'algorithme de Gauss. On notera r la dimension de ce noyau. V un vecteur du noyau qui ne soit pas dans la droite de ($1 \bmod P$) si il existe.

ⓘⓘⓘ Calcul d'un facteur. Posons $i = 1$; $B = \mathrm{pgcd}(\sigma(1) + V, P)$

Si $r = 1$
 Alors retourner P
Sinon Tant que $\deg(\mathrm{pgcd}(P; V - \sigma(i)))$ ⩽ 1
  $B \to \mathrm{pgcd}(P; V - \sigma(i+1))$
 Fin Tant que

Fin Sinon
Fin Si
Retourner P

⑤ Euclide étendu

Entrées : entiers positifs x et y
Sorties : entiers d, a, b avec $d = pgcd(x,y)$ et $ax + by = d$
Règles :

$$(x, y) \longrightarrow (x, 1, 0, y, 0, 1)$$

$$[u \neq 0] : (u, c, d, v, a, b) \longmapsto (v - qu ; a - qc ; b - qd ; u ; c ; d)$$

avec $q = v \div u$

$$[u = 0] : (u, c, d, v, a, b) \longmapsto (v, a, b)$$

⑥ Anthyphérèse

Entrées : entiers positifs x et y
Sorties : $pgcd(x, y)$
Règles : $[0 < u \leq v] : (u, v) \longmapsto (u ; v - u)$

$$[u > v] : (u, v) \longmapsto (v ; u)$$

$$[u = 0] : (u, v) \longmapsto v$$