Leçon N° 142 : PGCD et PPCM, algorithmes de calcul. Applications.

I) Cadre théorique.

1) Premières définitions.

Les anneaux sont supposés commutatifs et intègre et unitaires.

Définition 1 : Soient a et $b \in A$. On dit que a divise b, noté $a|b$ lorsqu'il $\exists c \in A$, $ac = b$.

Remarque 2 : Si $a|b$, on a alors $(b) \subset (a)$

Définition-Proposition 3 : La relation $a \mathcal{R} b$ ssi $(a|b$ et $b|a)$ est une relation d'équivalence appellée relation d'association. De plus, $a \mathcal{R} b$ ssi $\exists u \in A^\times$, $a = ub$.

Définition 4 : Soit $p \in A$, on dit que p est premier lorsque $p \in A^\times$ et lorsque $\forall (a,b) \in A^2$, $p|ab \Rightarrow (p|a$ ou $p|b)$.

Définition 5 : $p \in A$ est irréductible lorsque $p \in (A \setminus \{0\}) \setminus A^\times$ et lorsque $\forall (a,b) \in A^2$, $p = ab \Rightarrow a \in A^\times$ ou $b \in A^\times$.

Exemple 6 : Dans $\mathbb{Z}$, les irréductibles sont les $\pm p$ où $p \in \mathcal{P}$.

Proposition 7 : Si un élément est premier, alors il est irréductible.

Définition 8 :
- On dit que d est un pgcd de a et b lorsque : $d|a$, $d|b$ et $\forall x \in A$, $(x|a$ et $x|b) \Rightarrow x|d$.
- On dit que m est un ppcm de a et b lorsque : $a|m$, $b|m$ et lorsque $\forall x \in A$, $(a|x$ et $b|x) \Rightarrow m|x$.

Contre-exemple 9 : Le pgcd n'existe pas toujours ni le ppcm : Dans $\mathbb{Z}[i\sqrt{5}]$, 3 et $2+i\sqrt{5}$ n'ont pas de ppcm, et 3 et $3(2+i\sqrt{5})$ n'ont pas de pgcd.

Proposition 10 : Lorsqu'ils existent, deux pgcd et ppcm sont associés.

Définition 11 : a et b sont dits premiers entre eux lorsque $pgcd(a,b) = 1$.

2) Dans les anneaux factoriels

Définition 12 : A est dit factoriel lorsque A est intègre et
1) Tout $a \in A^*$ s'écrit sous la forme $u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ avec $u \in A^\times$, et $v_p(a)$ nuls sauf un nombre fini.
2) Cette écriture est unique une fois fixé $\mathcal{P}$ ce système de représentants irréductibles.

Proposition 13 : $a|b$ ssi $\forall p \in \mathcal{P}$, $v_p(a) \leq v_p(b)$.

Proposition 14 : Soient a et $b \in A$ factoriels a et b possèdent un pgcd et un ppcm : 1) Si $a = 0$, alors $pgcd(a,b) = b$
si $a = 0$ et $b = 0$, $ppcm(a,b) = 0$.
2) Si $a, b \in A^* / \sim$, $pgcd(a,b) = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$
$ppcm(a,b) = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$.

Corollaire 15 : $\forall (a,b) \in A$ factoriel, ab et $pgcd(a,b) \times ppcm(a,b)$ sont associés.

Théorème 16 : Soit A intègre vérifiant 1) de la déf 12. Il y a équivalence entre : 1) A vérifie 2 de déf 12.
2) Si $p \in A$ est irréductible et $p|ab$, alors $p|a$ ou $p|b$ (Euclide)
3) Si $a|bc$ et $a \wedge b = 1$, alors $a|c$ (Gauss).
4) p irréductible ssi p premier.

3) Dans les anneaux principaux.

Définition 17 : Soit A un anneau intègre, on dit que A est principal lorsque tout idéal de A est de la forme (a).

Proposition 18 : A principal $\Rightarrow$ A factoriel.

Exemples 19 : Tout corps est principal, $\mathbb{Z}$ et $\mathbb{K}[X]$ sont principaux, $\mathbb{K}$ étant un corps commutatif.

Contre exemple 20 : $\mathbb{K}[X,Y]$ factoriel non principal.

Leçon 1

Proposition 21 : $A[X]$ est principal ssi A est un corps.

Théorème 22 : (Bézout) Si A est principal. Soient $(a,b) \in A \setminus \{0\}$.
Alors $(a) + (b) = (a \wedge b)$
i.e. $\exists \lambda, \mu \in A$ tels que $a \wedge b = \lambda a + \mu b$.

Proposition 23 : Un anneau factoriel vérifiant Bézout est principal.

Théorème 24 : (Restes chinois). Soit A principal, $a_1, \dots, a_n$ 2-à-2 premiers entre eux. Alors $\varphi : A/(a_1 \times \dots \times a_n) \longrightarrow A/(a_1) \times \dots \times A/(a_n)$, $x \bmod (a_1 \dots a_n) \mapsto (x \bmod (a_1), \dots, x \bmod (a_n))$ est un isomorphisme d'anneaux.

Corollaire 25 : Soit $a \neq 0$ de décomposition $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$
Alors $A/(a) \simeq A/(p_1^{\alpha_1}) \times \dots \times A/(p_k^{\alpha_k})$

II) Anneaux euclidiens et algorithmes de calculs

Définition 26 : Un anneau A est dit euclidien lorsque A est intègre et lorsque $\exists \varphi : A \longrightarrow \mathbb{N}$ appelé stathme vérifiant :
1) $\forall a \in A, \forall b \in A \setminus \{0\}$, $\exists q, r \in A$ tels que $a = bq + r$ et $(r = 0$ ou $\varphi(r) < \varphi(b))$.
2) $\forall a, b \in A \setminus \{0\}$, $\varphi(b) \leq \varphi(ab)$

Exemples 27 : $\mathbb{Z}$ est euclidien pour le stathme $|\cdot|$
$\mathbb{K}[X]$ est euclidien pour le stathme $\deg$.

Proposition 28 : Soient $a, b \in A \setminus \{0\}$, $q, r \in A$ tels que $a = bq + r$,
alors $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(b,r)$.

Proposition 29 : Un anneau euclidien est principal.

Contre exemple 30 : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais pas euclidien.

Algorithme 31 : (Euclide) Entrée : a et b deux éléments de A euclidien non nuls
Initialisation : r est un reste de la D.E. de a par b.
Tant que $r = 0$:
  $a \longleftarrow b$
  $b \longleftarrow r$
  $r \longleftarrow$ un reste de la D.E. de a par b
Fin tant que
Sortie : renvoyer b.
Il se termine car la quantité b "diminue strictement"

Application 32 : $(X^a - 1) \wedge (X^b - 1) = X^{a \wedge b} - 1$.

Algorithme 32 : (Euclide étendu) Soient $a, b \in A \setminus \{0\}$ où A euclidien.
On considère (r_i) la suite des restes successifs obtenus par l'algorithme d'Euclide, avec $r_0 = a$ et $r_1 = b$.
On peut considérer deux suites (u_i) et (v_i) telles que $\forall i$,
$a u_i + b v_i = r_i$
Alors $\begin{cases} u_0 = 1 \\ u_1 = 0 \end{cases}$ $\begin{cases} v_0 = 0 \\ v_1 = 1 \end{cases}$
et $\forall i$ $\begin{cases} u_{i+2} = u_i - q_{i+2} u_{i+1} \\ v_{i+2} = v_i - q_{i+2} v_{i+1} \end{cases}$.

Lorsque l'algorithme se termine, on a u et v tels que $au + bv = a \wedge b$.

Application 33 : $a \in \mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si $a \wedge n = 1$.
On calcul son inverse en écrivant la relation de Bézout entre a et n.

Théorème 34 : (Lamé) $0 < y < x$ et $d = x \wedge y$.
Si l'algorithme d'Euclide se termine en n étapes, alors $x \geq d F_{n+2}$ et $y \geq d F_{n+1}$ où (F_n) est la suite de Fibonacci.

Proposition 35 : Le coût de l'algorithme d'Euclide est en $O(\log_2(y))$.

Proposition 36 : Soit $\mathbb{K}[X]$, son coût est en $O(d^\circ(A) \times d^\circ(B))$

III) Application :

1) Équations diophantiennes

Définition 37 : On appelle équation diophantienne, une équation d'inconnue $x \in \mathbb{Z}$ de la forme $ax \equiv b[n]$.

Théorème 38 : L'équation diophantienne $ax \equiv b[n]$ admet une solution ssi $a \wedge n | b$. Dans ce cas, si on note a' et n' /q, $a = (a \wedge n)a'$ et $n = (a \wedge n)n'$ et si on prend $x_0' \in \mathbb{Z}$, $a' x_0' \equiv 1 [n']$.
L'ensemble des solutions est $\{b' x_0' + kn' ; k \in \mathbb{Z}\}$ où $b = (a \wedge n) b'$.

Proposition 39 : On souhaite résoudre
$$\begin{cases} x \equiv a_1 [n_1] \\ \vdots \\ x \equiv a_r [n_r] \end{cases}$$
où $n_1, \dots, n_r$ sont premiers entre eux 2-à-2.
L'ensemble des solutions d'un tel système est $\{x_0 + kn, k \in \mathbb{Z}\}$ où $n = \prod_{i=1}^{r} n_i$ et x_0 sol particulière (obtenue par th chinois).

Exemple 40 : $\begin{cases} x \equiv 2 & [4] \\ x \equiv 3 & [5] \\ x \equiv 1 & [9] \end{cases}$ a pour solution $118 + 180\mathbb{Z}$.

2) Algèbre linéaire

Lemme 41 : (des noyaux) Soit $(P, Q) \in \mathbb{K}[X]^2$, $P \wedge Q = 1$.
Soient V un $\mathbb{K}$-ev de dimension finie et $f \in \mathcal{L}(V)$.
Alors $\ker(PQ(f)) = \ker(P(f)) \oplus \ker(Q(f))$.

Théorème 42 : (Dunford) Soit E un $\mathbb{K}$-ev de dim finie, soit $u \in \mathcal{L}(E)$ tel que χ_u soit scindé sur $\mathbb{K}$. Alors : $\exists! (d, n) \in \mathcal{L}(E)^2$ tel que
1) d diagonalisable sur $\mathbb{K}$.
2) n nilpotent
3) $d + n = u$
4) d et n commutent

De plus, d et $n \in \mathbb{K}[u]$.

3) Théorie des groupes

Lemme 43 : Si $(G, \cdot)$ un sous groupe commutatif, $r \geq 2 \in \mathbb{N}$ et $g_1, \dots, g_r$ des éléments 2-à-2 $\neq$ de G d'ordres respectifs $m_1, \dots, m_r$.
Alors $\exists g_0 \in G$ d'ordre $= \text{ppcm}(m_1, \dots, m_r)$.

Théorème 44 : Tout sous groupe fini du groupe multiplicatif $\mathbb{K}^*$, $\mathbb{K}$ étant un corps commutatif est cyclique.

Corollaire 45 : $\mathbb{U}_n(\mathbb{K}) = \{\lambda \in \mathbb{K}, \lambda^n = 1\}$ est un sous groupe cyclique de $\mathbb{K}^*$.

4) Critère d'Eisenstein

Définition 46 : Soit A factoriel et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$.
On définit le contenu de P par $c(P) = \text{pgcd}((a_i)_{i \in [\![0,n]\!]})$.
On dit que P est primitif lorsque $c(P) = 1$.

Lemme 47 : $c(PQ) = c(P)c(Q)$.

Théorème 48 : Les irréductibles de $A[X]$ où A factoriel sont :
1) Les constantes de A, irréductibles dans A.
2) Les $P \in A[X]$ de degré ≥ 1, primitifs et irréductibles dans $\mathbb{K}[X]$

Théorème 49 : (Eisenstein). Soit A factoriel et $P = \sum_{i=0}^{n} a_i X^i$.
S'il $\exists p \in A$ irréductible tel que : 1) $p \nmid a_n$
2) $p | a_i \quad \forall i \in [\![0, n-1]\!]$
3) $p^2 \nmid a_0$

Alors P irréductible dans $\mathbb{K}[X]$, donc dans $A[X]$ si $c(P) = 1$.

Théorème 50 : Si A factoriel, $A[X]$ factoriel.

Exemples 51 : Si p premier, $X^n - p$ irréductible dans $\mathbb{Z}[X]$
$\sum_{i=0}^{p-1} X^i$ irréductible dans $\mathbb{Z}[X]$