PGCD, PPCM dans les anneaux principaux.

Par Nicolas Lanchier [1]

1 Arithmétique dans les anneaux principaux.

Dans toute cette partie, A est un anneau, a et b deux éléments de A.

Définition 1.1 — On dit que a divise b s'il existe $c \in A$ tel que $b = a \cdot c$. Si de plus c est inversible, on dit que a et b sont associés. On notera $a \sim b$ cette relation. [3], Sect. 2.3

Proposition 1.2 — La relation de divisibilité est une relation d'ordre sur le quotient $A/\sim$. [3], Sect. 2.3

Théorème 1.3 — L'application $a \mapsto (a)$ induit un isomorphisme d'ensembles ordonnés de $A/\sim$ muni de la relation de divisibilité sur l'ensemble $\mathcal{I}(A)$ des idéaux principaux de A muni de l'inclusion inverse. [3], Sect. 2.3

Définition 1.4 — Un élément $p \in A$ est dit irréductible si $p \notin A$ et si $p = a \cdot b \ \Rightarrow \ a \in A^*$ ou $b \in A^*$. [3], Sect. 2.3

Définition 1.5 — On dit que a et b sont premiers entre eux si tout élément $d \in A$ divisant a et b est dans A^*. [3], Sect. 2.3

Proposition 1.6 — Si A est factoriel, l'ensemble $A/\sim$ est réticulé. Si $\inf\{(a),(b)\} = (c)$ et $\sup\{(a),(b)\} = (d)$, on pose $c = \text{ppcm}(a,b)$ et $d = \text{pgcd}(a,b)$. [3], Sect. 2.3

Proposition 1.7 — Si $c = \text{ppcm}(a,b)$ et $d = \text{pgcd}(a,b)$ alors les éléments $a \cdot b$ et $c \cdot d$ sont associés.

Théorème 1.8 (Bezout) — Si A est principal, a et b non nuls, et $d = \text{pgcd}(a,b)$ alors il existe u et v dans A tels que $d = a \cdot u + b \cdot v$. [3], Sect. 2.3

Théorème 1.9 (Gauss) — Soient a, b et c trois éléments d'un anneau factoriel. Si a divise $b \cdot c$ et si a et b sont premiers entre eux alors a divise c.

Théorème 1.10 (lemme d'Euclide) — Si p est irréductible et divise $a \cdot b$ alors p divise a ou b. [3], Sect. 2.3

2 Applications en algèbre.

Théorème 2.1 — Soient G_1, G_2, …, G_n des groupes cycliques d'ordres α_1, α_2, …, α_n respectivement. Alors le groupe $G = G_1 \times G_2 \times \ldots \times G_n$ est cyclique si et seulement si les α_i sont premiers deux à deux. [2], Sect. 1.2

Proposition 2.2 (lemme chinois) — Si p et q sont premiers entre-eux alors

$$\mathbb{Z}/p\,q\,\mathbb{Z} \ \cong \ \mathbb{Z}/p\,\mathbb{Z} \times \mathbb{Z}/q\,\mathbb{Z}$$

Théorème 2.3 — Pour $n \geq 3$, notons P_n le polygone régulier à n côtés. Alors P_n est constructible à la règle et au compas si et seulement si $n = 2^r\, p_1 \ldots p_s$ où les p_k sont des nombres premiers de Fermat deux à deux distincts. [1], exercice 4.15

THÉORÈME 2.4 (DÉCOMPOSITION DES NOYAUX) — Soient E un espace vectoriel, $f \in L(E)$ et $P = P_1\ P_2\ \ldots\ P_n \in K[X]$, les P_i étant premiers deux à deux. Alors

$$\operatorname{Ker} P(f) \ = \ \operatorname{Ker} P_1(f) \ \oplus \ \operatorname{Ker} P_2(f) \ \oplus \ \cdots \ \oplus \ \operatorname{Ker} P_n(f)$$

[2], Sect. 4.2

THÉORÈME 2.5 — Soient $f \in L(E)$ une application linéaire. Pour tout $x \in E$, notons P_x le polynôme unitaire de plus bas degré tel que $P_x(f)(x) = 0$ et posons $E_x = \{\, P(f)(x)\,;\, P \in K[X] \,\}$.

1. Si $E_x \cap E_y = \varnothing$ alors $P_{x+y} = \operatorname{ppcm}(P_x, P_y)$.
2. Si P_x et P_y sont premiers entre-eux alors $E_{x+y} = E_x \oplus E_y$.

THÉORÈME 2.6 — Un endomorphisme $f \in L(E)$ est dit semi-simple si pour tout sous-espace $F \subset E$ stable par f il existe un supplémentaire G de F stable par f.

1. Si π_f, le polynôme minimal de f, est irréductible alors f est semi-simple.
2. L'endomorphisme f est semi-simple si et seulement si π_f est produit de polynômes irréductibles unitaires deux à deux distincts.

[2], Sect. 4.5

3 Algorithmes de calcul.

DÉFINITION 3.1 — Soit A est un anneau factoriel et P un système de représentants des irréductibles de A. Alors tout $a \in A$ s'écrit $a = u \cdot \prod p^{\,\nu_p(a)}$ où p décrit P, $u \in A^*$ et où les $\nu_p(a)$ sont des entiers naturelles presque tous nuls. L'entier $\nu_p(a)$ est appelé valuation p-adique de a. [3], Sect. 2.3

PROPOSITION 3.2 — Soient $a,\ b \in A$. Alors a divise b si et seulement si pour tout $p \in P$, $\nu_p(a) \leq \nu_p(b)$. [3], Sect. 2.3

PROPOSITION 3.3 — Si $c = \operatorname{ppcm}(a, b)$ alors pour tout $p \in P$, $\nu_p(c) = \max(\nu_p(a), \nu_p(b))$. De même, si $d = \operatorname{pgcd}(a, b)$ alors $\nu_p(d) = \min(\nu_p(a), \nu_p(b))$. [3], Sect. 2.3

DÉFINITION 3.4 — Un anneau A est dit euclidien si

1. A est intègre et si
2. il existe une application $v : A \setminus \{0\} \longrightarrow \mathbb{N}$ appelée valuation telle que pour tout a et b non nuls il existe q et r dans A tels que $a = b \cdot q + r$ avec $r = 0$ ou $v(r) < v(b)$.

THÉORÈME 3.5 (ALGORITHME D'EUCLIDE) — Si A est un anneau euclidien, le pgcd de a et b est le dernier reste non nul dans la suite des divisions euclidiennes de a par b.

THÉORÈME 3.6 — Pour tout $r \in \mathbb{N}$, posons $\Gamma_r = \{\, P \in \mathbb{C}[X]\,;\, \deg P = r \,\}$. Alors pour tous n, $m \geq 1$, il existe une application continue $R : \Gamma_n \times \Gamma_m \longrightarrow \mathbb{C}$ appelée résultant telle que $R(P, Q) \neq 0$ si et seulement si P et Q sont premiers entre-eux. [2], Sect. 1.4

APPLICATION 3.7 — Soit D l'ensemble des matrices diagonalisables de $M_n(\mathbb{C})$. L'intérieur de D est l'ensemble des matrices dont les valeurs propres sont toutes distinctes. [2], Sect. 4.5

Références

[1] Hervé Francinou, Serge Gianella. *Exercices de mathématiques pour l'agrégation, algèbre 1.* Masson, 1995.

[2] Xavier Gourdon. *Les maths en tête. Algèbre.* Ellipses, 1994.

[3] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.