Szpirglas
Romaldi

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

On considère A un anneau commutatif intègre.

I - Notions de divisibilité, pgcd, ppcm

Définition 1.1 Soient $a, b \in A$. On dit que a divise b (ou b est multiple de a) s'il existe $c \in A$ tel que $b = ac$. On note alors $a \mid b$.

Proposition 1.2 Soient $a, b \in A$ alors a divise b si et seulement si $(b) \subset (a)$.

Définition 1.3 Soient $x, y \in A \setminus \{0\}$. On dit que d est un pgcd de x et de y si : d divise x et y et si tout autre diviseur commun divise d.
On dit que m est un ppcm de x et y si m est un multiple commun de x et de y et tout autre multiple commun est multiple de m.

Remarque 1.4 On peut définir de manière analogue le pgcd ou le ppcm d'un nombre fini d'éléments de A.

Proposition 1.5 Soient $x, y \in A \setminus \{0\}$ admettant un pgcd d alors l'ensemble des pgcd de x et y est dA^*, i.e. les éléments associés à d.

Exemple 1.6
dans $\mathbb{Z}[i]$, les pgcd de $2i$ et $-1+3i$ sont $1+i$, $1-i$, $-1+i$, $-1-i$.

Définition 1.7 Un anneau est dit à pgcd (resp. à ppcm) si tout couple d'éléments non nuls admet un pgcd (resp. un ppcm).

Proposition 1.8 (lemme de Gauss) Soit A anneau à pgcd et $a, b \in A$. Alors a et b sont premiers entre eux si et seulement si : $\forall c \in A,\ a \mid bc \Rightarrow a \mid c$

Proposition 1.9 (lemme d'Euclide) Supposons A anneau à pgcd et p irréductible de A.
Alors pour tout $x, y \in A$, $p \mid xy \Rightarrow p \mid x$ ou $p \mid y$.

Corollaire 1.10 Soit A anneau à pgcd. Alors pour tout a, a irréductible $\Leftrightarrow$ a premier.

II - Des anneaux à pgcd

1. Anneaux factoriels

Définition 2.1 On dit que A est factoriel s'il vérifie l'existence et l'unicité de la décomposition en facteurs irréductibles.

Théorème 2.2 (Gauss) Si A est factoriel alors $A[X]$ est factoriel.

Théorème 2.3 L'anneau A est factoriel si et seulement si : toute suite croissante d'idéaux principaux de A est stationnaire et irréductible équivaut à premier.

Définition 2.4 Soit A factoriel et $x \in A \setminus \{0\}$. On définit la valuation de x en p irréductible par $v_p(x) := \max\{n \in \mathbb{N} \mid p^n \mid x\}$.

Lemme 2.5 Soient $x, y \in A$ factoriel alors $x \mid y \iff \forall p \in \mathcal{P},\ v_p(x) \leq v_p(y)$.

Proposition 2.6 Soient A factoriel, $a = \prod_{p \in \mathcal{P}} p^{\alpha_p} \in A$ et $b = \prod_{p \in \mathcal{P}} p^{\beta_p} \in A$. Alors :
$d = \prod_{p \in \mathcal{P}} p^{\min(\alpha_p, \beta_p)}$ est un pgcd de a et b, et $m = \prod_{p \in \mathcal{P}} p^{\max(\alpha_p, \beta_p)}$ un ppcm.

Remarque 2.7 Ainsi, un anneau factoriel est à pgcd.

2. Anneaux principaux

Remarque 2.8 Un anneau principal est factoriel donc à pgcd.

Proposition 2.9 Soient A un anneau principal et $a, b \in A$. Alors un pgcd de a et b est un générateur de $(a) \cap (b)$.

D'autre part, un ppcm de a et b est un générateur de l'idéal $(a)+(b)$.

Théorème 2.10 (Bézout) Soient A anneau principal et $a, b \in A$. Alors a et b sont premiers entre eux si et seulement s'il existe $u, v \in A$ tels que $au + bv = 1_A$.

III - Calculs effectifs dans un anneau euclidien [Rom]

Définition 3.1 L'anneau A est dit euclidien, s'il existe un stathme φ tel que pour tous $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$.

Théorème 3.2 Un anneau euclidien est principal.
En particulier, c'est un anneau à pgcd.

Lemme 3.3 Soient $a, b \in A \setminus \{0\}$ avec A euclidien et r un reste de a par b.
Alors $a \wedge b = \begin{cases} b & \text{si } r = 0 \\ b \wedge r & \text{sinon} \end{cases}$ à un inversible près.

Application 3.4 (algorithme d'Euclide) Soient $a, b \in A \setminus \{0\}$ avec $\varphi(a) \geq \varphi(b)$.
On construit deux suites $(r_n)_{n \leq p}$ et $(q_n)_{n \leq p}$ d'éléments de A de la manière :

$a = q_1 r_0 + r_1 \quad (r_1 \neq 0, \varphi(r_1) < \varphi(r_0), r_0 = b)$

$r_0 = q_2 r_1 + r_2 \quad (r_2 \neq 0, \varphi(r_2) < \varphi(r_1))$

$\vdots$

$r_{p-3} = q_{p-1} r_{p-2} + r_{p-1} \quad (r_{p-1} \neq 0, \varphi(r_{p-1}) < \varphi(r_{p-2}))$

$r_{p-2} = q_p r_{p-1} + r_p \quad (r_p = 0)$

Alors :

$\forall k \in [\![0, p-1]\!], \exists u_k, v_k \in A, r_k = au_k + bv_k$

En particulier,

$a \wedge b = r_{p-1} = au_{p-1} + bv_{p-1}$

IV - Applications [Rom]

1. Le théorème chinois

On suppose que A est un anneau principal.

Théorème 4.1 Soit $(a_j)_{j \leq r}$ une famille d'éléments non inversibles de A, deux à deux premiers entre eux, et $a = \prod_{j=1}^{r} a_j$. L'application $\varphi : x \in A \longmapsto (\pi_j(x))_{j \leq R}$ est un morphisme d'anneaux surjectif de noyau (a). φ induit un isomorphisme $\overline{\varphi}$ d'inverse $\overline{\varphi}^{-1} : (\pi_j(x_j))_{j \leq R} \longmapsto \sum_{i=1}^{r} x_i u_i b_i \in A/(a)$, où $(u_j)_{j \leq r}$ vérifie $\sum_{j=1}^{r} u_j b_j = 1$.

développement 1

Application 4.2 Les solutions dans $\mathbb{Z}$ de $\begin{cases} u \equiv 1 \mod 3 \\ u \equiv 3 \mod 5 \\ u \equiv 0 \mod 7 \end{cases}$ sont $\{28 + 105k \mid k \in \mathbb{Z}\}$.

Application 4.3 La solution de degré minimal dans $\mathbb{Z}_5[X]$ de $\begin{cases} P(\bar{0}) = \bar{2} \\ P(\bar{1}) = \bar{0} \\ P(\bar{2}) = \bar{1} \end{cases}$ est $P = \bar{2} + \bar{4}X + \bar{4}X^2$

Application 4.4 Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i} \in \mathbb{N}^*$ alors $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$

2. Théorie des groupes

Lemme 4.5 Soit G un groupe commutatif fini. Alors l'exposant de G vaut le ppcm de l'ordre des éléments de G et est atteint comme ordre d'un élément.

Lemme 4.6 Soit G un groupe abélien fini et H sous-groupe de G. Tout élément de $\widehat{H}$ s'étend en un caractère de $\widehat{G}$.

développement 2

Théorème 4.7 Soit G un groupe abélien fini. Il existe alors $R \in \mathbb{N}^*$ et $d_1, \dots, d_R \geq 2$ vérifiant $d_i \mid d_{i+1}$ et $G \simeq \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_R}$.