PGCD et PPCM. Algorithmes de calcul. Applications.

A désigne un anneau commutatif, unitaire, intègre et $A \neq \{0\}$.

(I) Arithmétique dans un anneau factoriel

Soient $a, b \in A$.

1) Relation de divisibilité et éléments particuliers

Déf 1 : On pose $A^\times = \{u \in A : \exists v \in A, uv = 1\}$ l'ensemble des inversibles de A

Déf 2 : on dit que a divise b, noté $a|b$, si $\exists c \in A$ tq $b = ac$.

Prop 3 : On définit une relation d'équivalence sur A en posant : $a \mathcal{R} b \Leftrightarrow a|b$ et $b|a$.

Déf 4 : On dit que a et b sont associés si $a \mathcal{R} b$.

Prop 5 : On a : $a \mathcal{R} b \Leftrightarrow \exists u \in A^\times$ tq $a = bu$.

Déf 6 : On dit que $p \in A$ est irréductible si on a : $p \notin A^\times$ et $p = ab \Rightarrow a \in A^\times$ ou $b \in A^\times$.

Expl 7 : Dans $\mathbb{Z}$, les irréductibles sont les nombres premiers (positifs et négatifs).

Déf 8 : Un ensemble $\mathcal{P}$ d'irréductibles de A est un système de représentants irréductibles si pour tout p irréductible, $\exists ! \, q \in \mathcal{P}$ vérifiant $p \mathcal{R} q$.

Déf 9 : On dit que a et b sont premiers entre eux si : $\forall d \in A$, $d|a$ et $d|b \Rightarrow d \in A^\times$.

2) Anneau factoriel

Déf 10 : On dit que A est factoriel si : (E) $\forall a \in A^*$, $a = u \cdot \prod_{p \in \mathcal{P}} p^{v_p(a)}$, $u \in A^\times$, $v_p(a) \in \mathbb{N}^{(\mathcal{P})}$.
(U) cette écriture est unique

L'entier $v_p(a)$ est la valuation p-adique de a.

Expl 11 : $\mathbb{Z}$ est factoriel. Soit $\mathbb{K}$ un corps, alors $\mathbb{K}[X]$ est factoriel

Prop 12 : Si A est factoriel, alors $A[X]$ est factoriel. En particulier, $\mathbb{Z}[X]$, $\mathbb{K}[X,Y]$ st factoriels

Lemme d'Euclide : Si p est irréductible et $p|ab$ alors $p|a$ ou $p|b$

Lemme de Gauss : Si a divise bc et si a et b st premiers entre eux alors $a|c$

3) PGCD et PPCM

Prop 15 : Soient $a, b \neq 0$. Si $a|b$ alors $\forall p \in \mathcal{P}$, $v_p(a) \leq v_p(b)$

Déf 16 : Soient $a = u \cdot \prod_{p \in \mathcal{P}} p^{v_p(a)}$ et $b = v \cdot \prod_{p \in \mathcal{P}} p^{v_p(b)}$. On définit, à un inversible près,
$pgcd(a,b) = a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$ et $ppcm(a,b) = a \wedge b = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$

Prop 17 : On a : $\exists u \in A^\times$ tq $a \cdot b = u \cdot pgcd(a,b) \cdot ppcm(a,b)$

Prop 18 : Les application $\wedge : A^2 \to A$ et $\vee : A^2 \to A$ sont des LCI associatives et commutatives

Déf 19 : Soient $a_1, \dots, a_n \in A$. On définit par récurrence $pgcd(a_1, \dots, a_n)$ et $ppcm(a_1, \dots, a_n)$

4) Exposant d'un groupe fini

Déf 20 : Soit G un groupe fini. On note $N = \min\{n \in \mathbb{N} : \forall g \in G, g^n = e\} = \underset{g \in G}{ppcm} \; o(g)$ l'exposant de G.

D V ① **Th 21 :** Soit G un groupe abélien fini, alors $N = \max_{g \in G} o(g)$. En particulier, $\exists x \in G, N = o(x)$.

Th 22 : Soit G groupe abélien fini, alors $i : \begin{array}{l} G \to \hat{\hat{G}} \\ g \mapsto [\chi \mapsto \chi(g)] \end{array}$ est un isomorphisme de groupes.

D V ① **Classification des groupes abéliens finis :** Soit G un groupe abélien fini d'exposant $n_1 \in \mathbb{N}^*$ alors $\exists r \in \mathbb{N}^*$, $\exists n_1, \dots, n_r \in \mathbb{N}^*$ tq $n_1 | n_2 | \dots | n_r$ et $G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$

II Arithmétique dans un anneau principal

1) Anneau principal

Déf 24 : Soit $a \in A$. On note $(a) = \{ab, b \in A\}$ l'idéal engendré par a.

Prop 25 : On a : $b | a \iff (a) \subset (b)$. Par suite, $a \mathcal{R} b \iff (a) = (b)$.

Déf 26 : On dit que A est principal si tout idéal de A est engendré par un élément.

Exple 27 : $\mathbb{Z}$, $\mathbb{K}[X]$, $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ sont des anneaux principaux.

Prop 28 : Tout anneau principal est factoriel.

2) PGCD et PPCM

Soient $n \in \mathbb{N}^*$ et $(a_1, \dots, a_n) \in A^n$ avec A anneau principal.

Déf 29 : • $\bigcap_{i=1}^{n} (a_i)$ est un idéal de A. On appelle ppcm de $a_1, \dots, a_n$ tout générateur de cet idéal

• $\sum_{i=1}^{n} (a_i)$ est un idéal de A. On appelle pgcd de $a_1, \dots, a_n$ tout générateur de cet idéal

Prop 30 : On note $d = \text{pgcd}(a_1, \dots, a_n)$ et $m = \text{ppcm}(a_1, \dots a_n)$, déterminés à un inversible près

On a : $\forall i \in [\![1, n]\!]$, $d | a_i$ et $a_i | m$;

Tout diviseur de $a_1, \dots, a_n$ est un diviseur de d ;

Tout multiple de $a_1 \dots, a_n$ est un multiple de m.

Rq 31 : Les définitions de PGCD, PPCM dans un anneau factoriel et principal coïncident

Déf 32 : Les éléments $a_1, \dots, a_n$ sont (mutuellement) premiers entre eux si $\text{pgcd}(a_1, \dots, a_n) = 1$

DV ② Th de Sophie Germain : Soit p un nb premier impair tel que $q = 2p+1$ est premier.

alors il n'existe pas de solution $(x, y, z) \in \mathbb{Z}^3$ à l'équation $x^p + y^p + z^p = 0$ avec $xyz \not\equiv 0 [p]$

3) Théorème de Bézout

Th de Bézout : Soient $a, b \in A^*$. On note $d = \text{pgcd}(a, b)$, alors on a : $(a) + (b) = (d)$.

En d'autres termes : $\exists\, u, v \in A$ tq $au + bv = d$

Identité de Bézout : Soient $a, b \in A^*$. On a : $a \wedge b = 1 \iff \exists\, u, v \in A$ tq $au + bv = 1$

Appli 36 : Soient $(a, b) \in (\mathbb{Z}^*)^2$. On considère l'équation diophantienne : $ax + by = c$.

Si $\text{pgcd}(a, b) \nmid c$, l'équation n'admet pas de solutions ds $\mathbb{Z}$.

Si $\text{pgcd}(a, b) | c$, l'ensemble des solution est de la forme : $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + \frac{k}{a \wedge b} \begin{pmatrix} -b \\ a \end{pmatrix}, k \in \mathbb{Z}$.

4) Polynômes d'endomorphisme

Soit E un $\mathbb{K}$-ev de dimension finie et $u \in \mathcal{L}(E)$.

Lemme des noyaux : Soient $P_1, \dots, P_r \in \mathbb{K}[X]$, non nuls, 2 à 2 premiers entre eux et $P = \prod_{i=1}^{r} P_i$

alors $\text{Ker}(P(u)) = \bigoplus_{i=1}^{r} \text{Ker}(P_i(u))$

Déf - Prop 38 : $I_u = \{P \in \mathbb{K}[X] : P(u) = \tilde{0}\}$ est un idéal de $\mathbb{K}[X]$ principal,

donc il existe un unique polynôme unitaire μ_u tel que $I_u = (\mu_u)$.

Lemme : Soit $u \in \mathcal{L}(E)$. $\exists\, x \in E$ tq $\mu_u = \mu_{u,x}$ et alors $\langle x \rangle_u$ admet un supplémentaire stable.

Réduction de Frobenius : Soit $u \in \mathcal{L}(E)$. $\exists\, r \in \mathbb{N}^*$, $\exists\, P_1, \dots, P_r \in \mathbb{K}[X]$ unitaires, $\exists\, E_1, \dots, E_r$ stables

tq : $E = \bigoplus_{i=1}^{r} E_i$

• $\forall i \in [\![1, r-1]\!]$, $P_{i+1} | P_i$

• $\forall i \in [\![1, r]\!]$, u_{E_i} cyclique de polynôme minimal P_i

III) Arithmétique dans un anneau euclidien

1) Anneau euclidien

Déf 42 : On dit que A est euclidien si $\exists \varphi : A^* \to \mathbb{N}$, appelée stathme, tq $\forall a, b \in A^*$, $\exists (q, r) \in A^2$ tq $a = bq + r$ et ($r = 0$ ou $\varphi(r) < \varphi(b)$).

Exple 43 : $\mathbb{Z}$, $\mathbb{K}[X]$, $\mathbb{Z}[i]$, $\mathbb{Z}[j]$ sont des anneaux euclidiens

Prop 44 : Tout anneau euclidien est principal, à fortiori factoriel.

2) Algorithme d'Euclide

Prop 45 : Si $a = bq + r$, alors $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r)$

Algorithme d'Euclide : Soient $a, b \in A^*$. On pose $u_0 = a$ et $u_1 = b$.
On construit alors une suite $u_0, u_1, \dots$ grâce à l'algorithme suivant :
Supposons au rang $p \in \mathbb{N}^*$, $u_0, \dots, u_p$ construit.
Si $u_p = 0$, l'algorithme s'arrête ;
Sinon, on peut écrire $u_{p-1} = q_p \cdot u_p + u_{p+1}$ avec $u_{p+1} = 0$ ou $\varphi(u_{p+1}) < \varphi(u_p)$
Alors l'algorithme s'arrête pour un certain indice p_0 et $\mathrm{pgcd}(a, b) = u_{p_0 - 1}$

Rq 47 : Ds le cas où $(a, b) \in \mathbb{Z}^2$, $a > b > 0$. La complexité de l'algorithme est $O\left(\frac{\ln b}{\ln 2}\right)$.

Appli 48 : On peut déterminer un couple $(u, v) \in A^2$ tq : $au + bv = \mathrm{pgcd}(a, b)$.

Appli 49 : Soit (F_n) la suite de Fibonacci définie par : $F_0 = 0$, $F_1 = 1$, $\forall n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$, alors $\forall (m, n) \in \mathbb{N}^2$, $\mathrm{pgcd}(u_m, u_n) = u_{\mathrm{pgcd}(m,n)}$

Appli 50 : Soient $(a, b) \in \mathbb{N}^{*2}$. Dans $\mathbb{R}[X]$, on a : $\mathrm{pgcd}(X^a - 1, X^b - 1) = X^{\mathrm{pgcd}(a,b)} - 1$.

Exple 51 : Th de Wedderburn : Tout corps fini est commutatif.

3) Théorème des restes chinois

Th des restes chinois : Soit A anneau euclidien ; $a_1, \dots, a_n \in A$ 2 à 2 premiers entre eux
On note $p = a_1 \times \dots \times a_k$, alors

$$f : \begin{array}{ccc} A/pA & \longrightarrow & A/a_1A \times \dots \times A/a_nA \\ x \bmod pA & \longmapsto & (x \bmod a_1A ; \dots, x \bmod a_nA) \end{array}$$

est un isomorphisme

Appli 53 : Résolution de systèmes de congruences
Les solutions de $\begin{cases} x \equiv 2 \ [3] \\ x \equiv 3 \ [5] \\ x \equiv 2 \ [7] \end{cases}$ sont de la forme $23 + 105k$, $k \in \mathbb{Z}$

Appli 54 : Algorithme de Berlekamp
Soit $P = P_1 \dots P_r \in \mathbb{F}_p[X]$ le produit de r polynômes irréductibles 2 à 2 distincts
$\forall j \in [\![0, n-1]\!]$, soit $a_{0,j} + a_{1,j}X + a_{2,j}X^2 + \dots + a_{n-1,j}X^{n-1}$ le reste de la division de X^{jp} par P.
On note $A = (a_{i,j})_{0 \leq i,j \leq n-1}$
On a : $r = n - \mathrm{rg}(A - I)$
En particulier, si $r = 1$, P est irréductible