si possible plus de ppcm ★★

Soit A un anneau unitaire commutatif et intègre.

I) Anneaux à pgcd.

1) Divisibilité et anneaux factoriels

Définition 1 (R 7.1 L): $p \in A$ est dit irréductible si $p \neq 0_A$ et $p \notin A^\times$, et $\forall b, c \in A$ tq $bc = p$ alors $b \in A^\times$ ou $c \in A^\times$.

Définition 2 (R 7.2 L): Soient $a, b \in A$. a divise b ssi $(b) \subset (a)$

Définition 3 (R 7.1 L): Soit $p \in A^* \setminus A^\times$. p est premier si (p) est premier, i.e. si $\forall a, b \in A$ tq $ab \in (p)$, $a \in (p)$ ou $b \in (p)$.

Définition 4 (R 7.6 L): A est dit factoriel si tout élément $a \in A^* \setminus A^\times$ a une DPFI unique, à ordre et association près.

Exemple 5: dans $\mathbb{Z}$, $18 = 2 \times 3^2$

dans $\mathbb{R}[X]$, $X^2 - X - 6 = (X-3)(X+2)$

Proposition 6 (R 7.6 L): Dans A factoriel, a est premier ssi a est irréductible.

Contre-exemple 7: Dans $\mathbb{Z}[i\sqrt{2}]$ 2 est irréductible mais n'est pas premier.

2) Pgcd et anneaux à pgcd.

Définition 8 (R 8.2): Soit $r \geq 1$, $a_1, \dots a_r \in A^*$. On dit que ces éléments admettent un pgcd si il existe $\delta \in A^*$ tq $\forall k \in \{1, .., r\}$, $\delta | a_k$ et tout diviseur commun à $a_1, \dots a_r$ divise δ.

Définition 9: On dit que A est à pgcd si $\forall a, b \in A^*$ a et b admettent un pgcd.

Exemple 10: Dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$ ($\mathbb{K}$ un corps) deux éléments ont un pgcd. Ces anneaux sont à pgcd

Théorème 11 (R 8.2): un anneau factoriel est à pgcd. Précisemment, si $a = u \prod_{i=1}^{n} p_i^{\alpha_i}$ et $b = v \prod_{i=1}^{m} p_i^{\beta_i}$ où $u, v \in A^\times$, p_i sont irréductibles et non-associés et $\alpha_i, \beta_i \in \mathbb{N}$. on a alors $\delta = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}$

Application 12: $24 = 2^3 \times 3 \times 7^0$ et $84 = 2^2 \times 3 \times 7$

$\text{pgcd}(24; 84) = 2^2 \times 3 \times 7^0 = 12$.

Définition 13: si le pgcd de $a_1, \dots, a_r$ est inversible on dit qu'ils sont premiers entre eux dans leur ensemble.

Théorème 14: [Gauss] Dans un anneau à pgcd a et b sont premiers entre eux ssi $\forall c \in A^*$ $(a | bc \Rightarrow a | c)$.

Définition 15: $a_1, \dots, a_r \in A^*$ admettent un ppcm (unique (à association près)) si il existe $\mu \in A^*$ tq $\forall k \in \{1, \dots r\}$ $a_k | \mu$ et μ divise tout diviseur commun à $a_1, \dots, a_r$

Théorème 16 (R 8.2): A est à pgcd ssi $\forall a, b \in A^*$ a et b ont un ppcm. Dans ce cas $ab \overset{(*)}{=} \text{ppcm}(a;b)\,\text{pgcd}(a;b)$

Corollaire 17: si les $a_1, \dots, a_r$ sont premiers entre eux deux-à-deux alors $\text{ppcm}(a_1 \dots a_r) \overset{(*)}{=} a_1 \dots a_r$.

3) Anneaux principaux

Définition 18 (R 8.1): un anneau principal est un anneau dont tous les idéaux sont principaux i.e. tout idéal est engendré par un élément

Exemple 19: $\mathbb{Z}$ est principal.

(*) à association près

Proposition 8b: le pgcd est unique à association près.

Contre-exemple 20 : $I = \{P \in \mathbb{Z}[X] \mid 5 \mid P(0)\}$ n'est pas principal dans $\mathbb{Z}[X]$.

-R 8.1- **Théorème 21** : $A[X]$ est principal ssi A est un corps.

Proposition 22 : un anneau principal est factoriel

Exemple 23 : $\mathbb{R}[X]$ est factoriel (cf. exemple 5)

Proposition 24 : [identité de Bézout] un anneau principal est à pgcd. Pour $a_1, \dots, a_r \in A^*$ alors $\exists \delta \in A^*$ $(\delta) = (a_1) + \dots + (a_r)$ et donc il existe $u_1, \dots, u_r$ dans A tels que $\delta = u_1 a_1 + \dots + u_r a_r$.

R 8.2

Théorème 25 : [Bézout] Soit $a_1, \dots, a_r \in A^*$ où A est principal. $a_1, \dots, a_r$ sont premiers entre eux dans leur ensemble ssi il existe $u_1 \dots u_r$ tq $\sum_{i=1}^{r} u_i a_i = 1$.

Proposition 25 b : $\exists \mu \in A^*$ $(\mu) = (a_1) \cap \dots \cap (a_r)$. μ est le ppcm de $a_1, \dots, a_r \in A^*$

4) Anneaux Euclidiens

Définition 26 : un anneau A est dit euclidien si il est muni d'une division euclidienne, i.e si il existe un stathme φ tel que $\forall a, b \in A \times A^*$ $\exists q, r \in A$ tq $a = bq + r$ avec $r = 0_A$ ou, $r \neq 0$ $\varphi(r) < \varphi(b)$

R 9.1

q est le quotient et r le reste dans la division euclidienne de a par b.

Exemple 27 : $(\mathbb{Z}, \varphi_1)$ où $\varphi_1 : \mathbb{Z} \to \mathbb{N}$, $n \mapsto |n|$ est euclidien. $(\mathbb{R}[X], \varphi_2)$ où $\varphi_2 : P \mapsto \deg(P)$ est euclidien

Théorème 28 : un anneau euclidien est principal.

II. Algorithme de pgcd dans un anneau euclidien : A est euclidien

1) Division euclidienne :

Définition 29 : φ est croissant si $\forall a, b \in A^*$, $\varphi(ab) \geq \varphi(a)$

En particulier si $a \mid b$, $\varphi(b) \geq \varphi(a)$.

Proposition 30 : Dans un anneau euclidien (A, φ) on peut se ramener à $(A, \overline{\varphi})$ où $\overline{\varphi}$ est croissant

Théorème 31 : Soit (A, φ) un anneau euclien où φ est croissant. Alors :

1) $\forall a, b \in A^*$, $\varphi(ab) \geq \varphi(a)$, $\varphi(ab) = \varphi(a)$ ssi $b \in A^*$

En particulier, $\varphi(ab) > \varphi(a)$ pour $b \in A^* \setminus A^\times$

2) $\forall a \in A^*$, $\varphi(a) = \min_{x \in A^*} (\varphi(xa))$. Alors $\varphi(1_A) = \min_{x \in A^*} \varphi(a)$

3) $A^\times = \{a \in A^* \mid \varphi(a) = \varphi(1)\}$

R 9.1

Théorème 32 : Si A est euclidien, A est factoriel

2) Algorithme d'Euclide :

Proposition 33 : Soient $a, b \in A^*$, r le reste dans la division euclidienne de a par b. Alors

$$\text{pgcd}(a; b) = \begin{cases} b \text{ si } r = 0_A \\ \text{pgcd}(b; r) \text{ si } r \neq 0_A \end{cases}$$

à association près

Algorithme d'Euclide 34 : Soient a et $b \in A^*$ tels que $\varphi(a) > \varphi(b)$. On définit par récurrence une suite $(r_k)_k$ avec $r_0 = a$ et $r_1 = b$ et pour $k \geq 1$ si $r_k \neq 0_A$, r_{k+1} est le reste de la division euclidienne de r_{k-1} par r_k. On a alors $0 \leq \varphi(r_{k+1}) \leq \varphi(r_k)$

Il existe un entier $p \in \mathbb{N}$ tq $r_p = 0_A$ et on a $r_{p-1} = \text{pgcd}(a; b)$.

Application 35 : on utilise l'algorithme pour

Esc Exos 12.12 13.3

calcule pgcd(2652;2310) dans $\mathbb{Z}$ et pgcd(X^3+1; X^2+1) dans $\mathbb{R}[X]$. On trouve respectivement 6 et 1. Voir les étapes en annexe.

Théorème 36 : [Lamé] Soient $a, b \in \mathbb{Z}^2$. L'algorithme d'Euclide permet le calcul d'un pgcd dans $\mathbb{Z}$ entre a et b ($a > b \geq 1$) en moins de 5d divisions où d est le nombre de chiffres dans l'écriture décimale de b.

Esc Exo 12.4

3) Euclide étendu :

Proposition 37 : on peut, en remontant l'algorithme d'Euclide, trouver les facteurs de l'identité de Bézout

Esc Exo 13.3

Application 38 : En reprenant l'exemple 35, on a $-27 \times 2652 + 31 \times 2310 = 6$

et $\frac{X+1}{2}(X^3+1) + \frac{1-X-X^2}{2}(X^2+1) = 1$

III. Applications :

1) Lemme des noyaux :

R. 19.4

Théorème 39 : soit $p \geq 2$, $P_1, \dots, P_p \in \mathbb{K}[X]^*$ ($\mathbb{K}$ un corps) deux-à-deux premiers entre eux et $P = \prod_{k=1}^{p} P_k$. Alors pour $u \in \mathcal{L}(E)$, E e.v de dimension finie : $\ker(P(u)) = \bigoplus_{k=1}^{p} \ker(P_k(u))$.

2) Congruences et restes chinois :

R 7.4

Définition 40 : soit $I \in A$, un idéal, $a, b \in A$. a est dit congru à b modulo I dans A si $b-a \in I$. On note $a \equiv b \mod I$

Exemple 41 : dans $\mathbb{Z}$, $12 \equiv 4 \mod [8]$

Proposition-définition 42 : la relation de congruence est une relation d'équivalence sur A. On note A/I l'ensemble des classes d'équivalence modulo I.

Exemple 43 : $12 \equiv 4 \mod 8$, $\overline{12} = \overline{4}$ dans $\mathbb{Z}/8\mathbb{Z}$

R 7.4

Théorème 44 : [restes chinois] Soit A un anneau principal. $a_1, \dots, a_r \in A^*$. si les $a_1 \dots a_r$ sont premiers entre eux deux-à-deux alors $A/(a_1 \dots a_r) \cong A/(a_1) \times \dots \times A/(a_r)$

DVT 1

R 8.3

Esc 19.8

Application 45 : [Sunzi] Soient des objets en nombre inconnus. Si on les compte par 3 il en reste 2; par 5, il en reste 3; par 7, il en reste 2. Combien y a-t-il d'objets ?

Esc

Exercice 46 : Existe-t-il des entiers x et y tels que $x^2 - 2y^6 = 17$?

Application 47 Polynôme interpolateur de Lagrange Esc 15.8

3) Étude des polynômes :

R 12.11

Définition 47 : le contenu d'un polynôme $P(X) = \sum_{k=0}^{n} a_k X^k$ de $\mathbb{Z}[X] \setminus \{0\}$ est $c(P) = \text{pgcd}(a_1, \dots a_n)$

Définition 48 : un polynôme non-nul est dit primitif si son contenu vaut 1.

Proposition 49 : le produit de polynômes primitifs est primitif

Proposition 50 : [Gauss] $\forall P, Q \in \mathbb{Z}[X]^*$, $c(PQ) = c(P)c(Q)$

Théorème 51 : [Eisenstein] $P(X) = \sum_{k=0}^{n} a_k X^k$ non constant dans $\mathbb{Z}[X]$. Si il existe p premier tq p ∤ a_n, p | a_i $\forall i \in \{1 \dots n\}$, $p^2 \nmid a_0$. P est irréductible dans $\mathbb{Q}[X]$

DVT

Proposition 51 : $P(X+1)$ irréd. ssi $P(X)$ irréd.

→ rapproches III.1) de III.3)

Références : [R] - Jean-Étienne Rombaldi "Mathématiques pour l'agrégation, algèbre et géométrie"

[Esc] - Jean-Pierre Escofier "Toute l'algèbre de la licence"

Application 35 : détails de l'algorithme

- $2652 = 1 \times 2310 + 342$
  $2310 = 6 \times 342 + 258$
  $342 = 1 \times 258 + 84$
  $258 = 3 \times 84 + 6$ ⑥ pgcd
  $84 = 14 \times 6 + 0$
- $X^3+1 = X(X^2+1) + (-X+1)$
  $X^2+1 = (-X-1)(-X+1) + 2$ ② pgcd
  $-X+1 = \frac{-X+1}{2} \times 2 + 0$

Le pgcd étant défini à association près on peut choisir $(X^3+1) \wedge (X^2+1) = 1$.

Application 38 : algorithme "remonté"

- $6 = 258 - 3 \times 84 = 258 - 3 \times (342 - 258)$
  $= 4 \times 258 - 3 \times 342$
  $= 4 \times (2310 - 6 \times 342) - 3 \times 342$
  $= 2310 \times 4 - 27 \times (2652 - 2310)$
  $= -27 \times 2652 + 31 \times 2310$
- $2 = X^2+1 + (X+1)(-X+1)$
  $= X^2+1 + (X+1)(X^3+1 - X(X^2+1))$
  $= (X+1)(X^3+1) + (1-X-X^2)(X^2+1)$

Anneaux et résultats liés au pgcd / ppcm

Anneaux à pgcd

- Lemme de Gauss,
- Existence du ppcm et unicité à association près
- Existence et unicité du pgcd à association près

↓

Anneaux factoriels

- identification du pgcd avec la DPFI.

↓

Anneaux principaux

- Identité et théorème de Bézout
- Théorème des restes chinois

↓

Anneaux euclidiens :

- Division euclidienne · Algorithmes de pgcd

$\mathbb{Z}[i\sqrt{5}]$ n'est pas à pgcd. 9 et $3(2+i\sqrt{5})$ n'ont pas de pgcd.

$\mathbb{Q}^+[X]$ est un anneau à pgcd ni factoriel ni principal.