142 : PGCD - PPCM ← je t'aime pas 😊

I) Notion de PGCD - PPCM

A) 1ère déf :

(rajouter des exs...)

[GRAS] p. 217 - ~~déf : a|b + irréd. ex sur ℤ~~ + ~~[déf pgcd/ppcm avec ∧ (+ thm 2.8...) + exs sur ℤ]~~ ?

- [BER] p. 517 - 523 (sans étranger ; déf élément 1er ? sinon à peu près tout.)
  ↳ déf pgcd/ppcm avec |

B) PGCD - PPCM dans un anneau factoriel

- [BER] p. 544 - 549 (sans parler d'élément normalisé) + rajouter contenu et CNS P irréd sur A[X] (+ loin dans BER)
  + thm : A fact ⇒ A[X] fact ♥ y penser

C) Cas des anneaux principaux

[BER] p. 526 - 531 (sans : thm chinois ; thm 2.10 ni scri vu en fact ?)
+ P. 549 : principal ⇒ factoriel + rem ⇐ faux ℤ[X] [donner des exs de A principaux]
+ rem : Bézout utile pour trouver des inverse dans des anneaux quotient + donner ex dans $\mathbb{Z}/n\mathbb{Z}$ et $\frac{\mathbb{Z}[X]}{(P)}$ ...
Appli : Dév lemme des noyaux + diagonalisat° ♥

Dév 1] [RON]

II) Cas des anneaux euclidiens :

A) Anneaux euclidiens :

[PER] p. 50 - 54

déf : anneau eucli (rem : pas unicité) + exs : ℤ, ℤ[i]
Thm : eucli ⇒ principal + rem ⇐ faux : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ ← p. 54 et +
Lemme : div eucli sur A[X] ↳ rem sur ℤ[X] si P unitaire] et en + unicité ♥
Thm : K corps ⇒ K[X] eucli + rem : unicité

B) Algo d'Euclide et csq :

[RON] + [PER]

- [RON] p. 264 - 265 : lemme + explicat° algo Euclide
  ~~→ Rem : on a déjà pgcd = inv~~
  Thm : il s'arrête et r_p = pgcd... → voir complexité dans [CAL. Alg] rien compris
- [BER] p. 534 - 539 : explicat° algo étendu avec u_i, v_i
  Thm : → relat° de Bézout + explicat° avec tableau

[BER] Ex dans ℤ[i]

♥ Rem : dans ℝ[X] en général on pose la division eucli ...
+ ↳ dans K[X] avec algo euclide on a pgcd = inv par extension de corps
+ rem : compter la complexité dans le pire des cas... (pour K[X] en fct de d°P...)
← faudrait trouver ça qq part... mais où ?

III) Applications aux équations arithmétiques

A) Systèmes de congruence :

[RON] [BER]
- [RON] p. 249 + 286 + 290 - 291 → éq dioph. ax = b [n] thm 1.9.13
→ Thm chinois dans A principal
→ Reformulation sur ℤ
→ Appli : résolut° d'un système d'éq dioph → pour trouver une solut° part.
Ex...
+ Thm : système de 2 éq dioph qd $n_1 \wedge n_2 = 1$

(trouver meilleur titre)

B) Résolution d'éq dioph grâce au pgcd dans d'autres anneaux que ℤ...

[PER]
- [PER] p. 56 - 58 : explique but $\Sigma = \{a^2+b^2 \mid a,b \in \mathbb{N}\}$ + tout sur ℤ[i] thm des 2 carrés + csq : irréductibles de ℤ[i]

- [CAL. Alg] ... ou [101 dév] → éq de Mordell $x^2+2 = y^3$ → tout sur $\mathbb{Z}[i\sqrt{2}]$ + résolue

Dév 2

les 101 dév...

(parce qu'on parle de valuat° p-adique...)

Réf : [BER] - [RON] - [PER] ([CAL. Alg] ou [101 dév...])