Plan détaillé $\boxed{122}$ suite

III) Applications :

A) Algèbre linéaire : E ev. de dim finie, $u \in \mathcal{L}(E)$

[ROM] p. 603

Rem$_{37}$: La principalité et factorialité de $\mathbb{K}[X]$ permet d'avoir beaucoup de propriétés sur l'algèbre $\mathbb{K}[u] = \{P(u) \mid P \in \mathbb{K}[X]\}$

[ROM] p. 604 – 606

Prop-déf$_{38}$: $I_u = \{P \in \mathbb{K}[X] \mid P(u) = 0\}$ est un idéal non nul de $\mathbb{K}[X]$, donc il admet un unique générateur unitaire. On le note π_u, c'est le polyn. min de u.

THM$_{39}$: dim de $\mathbb{K}[u] \rightsquigarrow \mathbb{K}[u] \simeq \mathbb{K}[X]/(\pi_u)$

THM$_{40}$: $\mathbb{K}[u]$ corps $\iff \mathbb{K}[u]$ intègre $\iff \pi_u$ irréductible.

[ROM] p. 609 – 610

Lemme$_{41}$: lemme avant déc. des noyaux

THM$_{42}$: Lemme de déc. des noyaux

Appli$_{43}$: critère de diagonalisation.

Dév 1

B) Anneau des entiers de Gauss :

[PER] p. 56 – 58

On note $\Sigma = \{n \in \mathbb{N} \mid n = a^2 + b^2, (a,b) \in \mathbb{N}^2\}$.

Ex$_{44}$: $0, 1, 2, 4, 5 \in \Sigma$.

Déf$_{45}$: $\mathbb{Z}[i]$: anneau (ss-anneau de $\mathbb{C}$) + application "norme". $N : z \in \mathbb{Z}[i] \mapsto z\bar{z}$

Prop$_{46}$: N multiplicative.

Prop$_{47}$: $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. + $z \in \mathbb{Z}[i]^\times \iff N(z) = 1$.

Prop$_{48}$: Σ stable par multiplication.

Prop$_{49}$: $\mathbb{Z}[i]$ euclidien, de stathme N) ⑦

Lemme$_{50}$: -1 carré dans $\mathbb{F}_p$ $\iff$ $p = 2$ ou $p \equiv 1 [4]$. (p 1er)

[PER] ou [ROM] p. 269

Lemme$_{51}$: p 1er, $p \in \Sigma \iff p$ réductible dans $\mathbb{Z}[i]$.

THM$_{52}$: $p \in \mathbb{N}$ 1er, $p \in \Sigma \iff p = 2$ ou $p \equiv 1 [4]$.

THM$_{53}$: $n \in \mathbb{N}^*$, $n \in \Sigma \iff \forall p$ 1er tq $p \equiv 3 [4]$, $v_p(n)$ pair

Dév 2

Cor$_{54}$: les irréductibles de $\mathbb{Z}[i]$ sont les $p \in \mathcal{P}$ tq $p \equiv 3 [4]$ + $a + ib$ tq $a^2 + b^2 \in \mathcal{P}$ ⑧

C) Théorème chinois :

[ULM] p. 55 – 58 (regarder algo de Gauss ?)

Déf$_{55}$: idéaux étrangers : $I + J = A$

THM$_{56}$: thm chinois : $I_1, \dots, I_n$ idéaux étrangers 2 à 2, $I = I_1 \cap \dots \cap I_n$

$$\varphi : \begin{array}{l} A/I \longrightarrow A/I_1 \times \dots \times A/I_n \\ \bar{x} \longmapsto (x + I_1, \dots, x + I_n) \end{array} \text{ isomorphisme}$$

Rem$_{57}$: Dans un anneau principal, les idéaux I_j sont de la forme $I_j = (m_j)$ et $(m_i), (m_j)$ étrangers $\iff m_i, m_j$ 1ers entre eux

Cor$_{58}$: A principal thm chinois

[ROM] p. 291

Ex$_{59}$: $\begin{cases} k \equiv 2 [4] \\ k \equiv 3 [5] \\ k \equiv 1 [9] \end{cases} \rightsquigarrow$ solut° $k = 838 + 180q \quad q \in \mathbb{Z}$
$= 118 + 180q' \quad q' \in \mathbb{Z}$ ⑨

Réf :

[ROM] - Rombaldi - Maths pour l'agreg, Algèbre

[PER] - Perrin - Cours d'algèbre

[ULM] - Ulmer - Anneaux, corps, résultants

Plan détaillé $\boxed{122}$ Anneaux principaux

- A anneau commutatif. On note $A^\times$ son groupe des inversibles

I) Notion de principalité

A) Idéaux et anneaux principaux :

Déf1 : idéal

Ex2 $\{0\}$, A, $\mathrm{Ker}(\varphi)$ pour φ morphisme d'anneaux

Déf2 idéal premier + idéal maximal

Thm3 : équivalences idéal 1^{er}/max $\Leftrightarrow$ A/I intègre/corps + p premier $\Leftrightarrow (p)$ 1^{er} (sans le pt 5)

Déf4 : idéal + anneau principal

Ex5 $n\mathbb{Z}$ idéal principal, $\mathbb{Z}$ principal, corps principal, $\mathbb{K}[X]$ où $\mathbb{K}$ corps commut.

Prop6 : Dans un anneau principal, tout idéal non nul et premier est maximal

Prop7 : On suppose A intègre, $\boxed{A[X] \text{ principal} \Leftrightarrow A \text{ corps}}$ ← à mettre car utilise anneaux eucli

[ROM] p.235 · [ROM] p.223 · [ROM] p.237 · ou [ULM] p.42 · [ROM] p.242

B) Exemple important : Anneaux euclidiens :

Déf8 Anneau euclidien + stathme

~~THM9 Un ann~~

Ex9 $\mathbb{Z}$ avec $|\cdot|$ (rem quotient, reste non unique) ; $\mathbb{K}[X]$ avec $\deg(\cdot)$

THM10 Anneau euclidien est principal

Rem11 Réciproque fausse : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ ③

[FCR] p.50 · [FCR] p.54

II) Arithmétique dans les anneaux principaux :

A) Divisibilité et irréductibilité :

Prop12 : $a|b \Leftrightarrow (b) \subseteq (a)$

Déf13 éléments associés $a\sim b \Leftrightarrow a|b$ et $b|a \Leftrightarrow (b)=(a)$

Prop14 : $a\sim b \Leftrightarrow \exists u \in A^\times, a = ub$

Déf15 élément premier entre eux (tt diviseur commun est inversible)

Déf16 élément irréductible

Prop17 : A anneau principal, premier $\Leftrightarrow$ irréductible.

Ex18 sur $\mathbb{Z} \rightsquigarrow \pm p$, p 1^{er}

THM18 : A principal, $(a) \subseteq A$ maximal $\Leftrightarrow$ a irréductible dans A.

[ULM] p.39–41 · [ULM] p.45–46

B) PGCD - PPCM :

[ULM] p.40–44

Déf19 : pgcd, ppcm

Ex20 : un pgcd de 20, 15 est 5 ; un pgcd de X et Y dans $\mathbb{K}[X,Y]$ est 1

Rem21 : · pgcd/ppcm pas unique, associés, dans $\mathbb{K}[X]$ (unitaire) / $\mathbb{Z}$ ($\in \mathbb{N}$)

· a, b 1^{er} entre eux, $\mathrm{pgcd}(a,b) \sim 1$

Prop22 : dans anneau principal $a, b \neq 0$, c est un ppcm de $a, b \Leftrightarrow (a)\cap(b) = (c)$

pgcd — $\Leftrightarrow$ $(a,b) = (d)$

Rem23 : gén pour + d'élément

THM24 : décomposition de Bézout : $(d) = (a_1, \dots, a_m) \rightsquigarrow \exists (b_1, \dots, b_m)$ tq $d = a_1b_1 + \dots + a_mb_m$.

Rem25 : En pratique on réalise les calculs dans un anneau euclidien

Algorithme d'Euclide 26 : ... l'algo s'arrête car $(\varphi(r_i))_i$ strictement ↘ et ≥ 0, le dernier reste non nul est le pgcd

Rem27 : En utilisant (="remontant") l'algo d'Euclide, on trouve une relat° de Bézout.

THM28 : Lemme d'Euclide + lemme de Gauss

C) Lien avec les anneaux factoriels.

[ULM] p.63–67

Déf29 : anneau factoriel + système de représentants et valuations

Dans la suite de la partie A factoriel, $\mathcal{P}$ système de rep. des irréd.

Prop30 : $a|b \Leftrightarrow v_p(a) \leq v_p(b)$ $\forall p \in \mathcal{P}$

· $g = \prod p^{\min(v_p(a), v_p(b))}$ est un pgcd + autre déf des ppcm

Rem31 : Lemmes d'Euclide + Gauss encore valables

Prop32 : Toute suite ↗ d'idéaux est stationnaire (Anneau principal)

THM33 : A principal alors A factoriel

[FCR] p.47–48

Ex34 : $\mathbb{Z}$ factoriel avec $\mathcal{P}$ = nbre 1^{er} ≥ 0, $\mathbb{R}[X]$ avec $\mathcal{P}$ = polyn. unit irréd.

Rem35 : Unicité ⚠ $\mathbb{Z}[i\sqrt{5}]$ non factoriel : $6 = (1+i\sqrt{5})(1-i\sqrt{5}) = 3\times 2$ or les 3 sont irréductibles.

Rem36 : On a la suite d'implications : A corps ⇒ A euclidien ⇒ A ~~factoriel~~ principal ⇒ A factoriel