

L.122 Anneaux principaux. Exemples et application

I. Anneaux Principaux:

1) Généralités:

Définition 1: soit A un ensemble muni de deux lois

internes notées "+" et "·". $(A, +, \cdot)$ est un anneau si

i) $(A, +)$ est un groupe abélien

ii) "·" est associative

iii) "·" est distributive par rapport à "+".

Si "·" a un élément neutre 1_A l'anneau est dit

unitaire. Si "·" est commutative, l'anneau

est dit commutatif.

Exemples 2: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}[X], +, \cdot)$ commutatif

$(M_n(\mathbb{K}), +, \cdot)$, $(\mathbb{Z}(E), +, \cdot)$ non commutatifs

$(\mathbb{N}, +, \cdot)$ n'est pas un anneau.

Dans la suite $(A, +, \cdot)$ désigne un anneau commutatif

Définition 3: $a \in A^*$ est un diviseur de zéro s'il existe

$b \in A$ tel que $b \neq 0$ et $ab = 0$.

Exemple 4: dans $\mathbb{Z}/6\mathbb{Z}$ $\bar{3} \cdot \bar{2} = \bar{0}$

Définition 5: A est intègre si il n'a pas de diviseur

de zéro. Autrement dit $(a \neq 0, b \neq 0 \Rightarrow ab \neq 0)$

Exemple 6: $M_n(\mathbb{R})$ est un anneau non intègre

Définition 7: Soit $I \subset A$. I est un idéal de A si

i) $(I, +)$ est un sous-groupe de $(A, +)$

ii) $\forall (x, a) \in I \times A, ax \in I$.

Proposition 8: une intersection d'idéaux est un idéal

Une somme finie d'idéaux est un idéal.

Définition 9: un idéal I de A est dit principal s'il

est engendré par un élément $x \in A$. On note $(x) = I = xA$.

Définition 10: un anneau est dit principal si tous ses idéaux sont principaux.

Exemple 11: $(\mathbb{Z}, +, \cdot)$ est principal, $(\mathbb{R}[X], +, \cdot)$ est principal. $(\mathbb{Z}[X], +, \cdot)$ n'est pas principal.

2) Divisibilité dans les anneaux:

Dans la suite A est un anneau unitaire, commutatif, intègre.

Définition 12: $p \in A^* \setminus A^*$ est irréductible si, pour $a, b \in A$ tq $ab = p$ alors a ou b est inversible.

Définition 13: $p \in A^* \setminus A^*$ est premier si (p) est premier i.e. si $\forall a, b \in A$ tq $ab \in (p)$ alors $a \in (p)$ ou $b \in (p)$.

Notation 14: p a s'écrit $(a)(c)$ en terme d'idéaux.

Remarque 15: Dans \mathbb{Z} la notion de premier est d'irréductible est équivalente.

Définition 16: l'anneau A est factoriel si tout $a \in A^* \setminus A^*$ admet une décomposition en produit de facteurs irréductibles, unique à association près.

Exemple 17: $(\mathbb{Z}, +, \cdot)$ est factoriel

Théorème 18 (Gauss): A est factoriel ssi il est intègre

et toute suite croissante d'idéaux de A est stationnaire et tout élément irréductible est premier.

Corollaire 19: dans A factoriel, un élément est irréductible ssi il est premier.

Corollaire 20: A principal implique A factoriel

3) Lien entre ces structures d'anneaux:

Définition 21: soient A et A' deux anneaux. On

[X6
29]

[X6
29]

[X6
30]

appelle morphisme d'anneaux $f: A \rightarrow A'$ une application telle que $\forall x, y \in A \quad f(x+y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$. et $f(1) = 1$

Proposition 22: le noyau d'un morphisme d'anneaux est un idéal.

Proposition 23: Soit I un idéal de A . De même que pour les groupes on peut déf. l'anneau quotient A/I .

Exemple 24: $\forall n \geq 1 \quad n\mathbb{Z}$ est un idéal de \mathbb{Z} . On définit alors l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$.

Théorème 25: Soit $f: A \rightarrow A'$ un morphisme d'anneaux $\varphi: A/\ker(f) \rightarrow \text{Im}(f)$ est un isomorphisme d'anneaux.

Théorème 26: \mathbb{Z} est premier ssi A/I est intègre. \mathbb{Z} est maximal ssi A/I est un corps. (\mathbb{Z} est maximal si les seuls idéaux qui contiennent I sont A et I).

Théorème 27: $A[X]$ principal ssi A est un corps. Application 28: $(\mathbb{R}[X], +, \cdot)$ est principal, $(\mathbb{Z}[X], +, \cdot)$ non.

II. Arithmétique dans les anneaux:

1) Anneaux à pgcd: Définition 29: Des éléments a_1, \dots , ou non-nuls de A admettent un pgcd si il existe $\delta \in A^*$ tel que $\forall k \in \{1, \dots, r\} \quad \delta | a_k$ et tout diviseur commun aux a_k divise δ . Il est unique à association près.

Définition 30: Les éléments admettent un ppcm si il existe $\mu \in A^*$ tel que $\forall k \in \{1, \dots, r\} \quad a_k | \mu$ et μ divise tout multiple commun aux a_k . Il est

unique à association près. Définition 31: A est à pgcd si deux éléments de A^* admettent toujours un pgcd.

Théorème 32: un anneau factoriel est à pgcd. Corollaire 33: un anneau principal est à pgcd.

Exemple 34: $K[X]$ est à pgcd, \mathbb{Z} est à pgcd.

Théorème 35: [Gauss] A un anneau à pgcd. Deux éléments non-nuls sont premiers entre eux ssi $\forall c \in A^* \quad a | bc \Rightarrow a | c$.

Théorème 36: [Euclide] si $a | bc$ et a irréductible alors $a | b$ ou $a | c$.

Proposition 37: A est à pgcd ssi $\forall a, b \in A^*, a \wedge b$ admettent un ppcm. On a alors $ab = \text{pgcd}(a, b) \text{ppcm}(a, b)$.

2) dans un anneau principal: Théorème 38: [Bézout] Soit a_1, \dots un des éléments non-nuls premiers entre eux dans leur ensemble (i.e. leur pgcd est inversible) alors il existe $(u_1, \dots, u_r) \in A$ tq $u_1 a_1 + \dots + u_r a_r = 1$.

Théorème 39: [Restes Chinois] Dans A principal, si a_1, \dots or sont premiers entre eux deux-à-deux alors $A/(a_1, \dots, a_r) \cong A/(a_1) \times \dots \times A/(a_r)$

3) Le cas des anneaux euclidiens: Définition 40: un anneau est euclidien s'il existe φ un scalaire tq $\forall (a, b) \in A^2, \exists (q, r) \in A^2$ tel que

Définition 37b: Des éléments a_1, \dots or sont premiers entre eux si leur pgcd est inversible. Proposition 37t: si a_1, \dots , or sont premiers entre eux deux-à-deux $\text{ppcm}(a_1, \dots, a_r) = a_1 \dots a_r$

[XG] 30

[Ro] 216

[Ro] 236

[Ro] 237

[Ro] 240

[Ro] 238

[DP] 48

[Ro] 243

(2)

$a = bq + r$ et $r = 0$ ou $r \neq 0$ et $\varphi(r) < \varphi(b)$.

Exemples 40: \mathbb{Z} et $\mathbb{R}[X]$ sont euclidiens pour les

statutues $\varphi_{\mathbb{Z}}: \mathbb{Z} \rightarrow \mathbb{Z}$ et $\varphi_{\mathbb{R}[X]}: P \rightarrow \deg(P)$

Proposition 41: un anneau euclidien est principal

Proposition 42: Soient $a, b \in A^* \setminus \{0\}$ euclidien et r un reste dans la division euclidienne de a par b . Alors

$$a \wedge b = \begin{cases} b & \text{si } r = 0 \\ br & \text{si } r \neq 0 \end{cases}$$

Algorithme 43: on définit $(r_n) \in \mathbb{N}$ une suite d'éléments de A telle que $r_0 = b, \forall m \geq 2, r_m$ est le reste dans la division euclidienne de r_{m-2} par r_{m-1} , ou 0 si $r_{m-1} = 0$. Le dernier reste non nul est le pgcd de a, b .

Application 44: $2652 \wedge 2310 = 6$ dans \mathbb{Z}
 $(X^3+1) \wedge (X^2+1) = 1$ dans $\mathbb{R}[X]$

Algorithme 45: en "remontant" l'algorithme d'Euclide on trouve les facteurs de l'identité de Bezout

Application 45: $-27 \times 2657 + 31 \times 2310 = 6$ dans \mathbb{Z}
 $\frac{X+1}{2} \times (X^3+1) + \frac{X^2-X+1}{2} (X^2+1) = 1$ dans $\mathbb{R}[X]$

III. Applications:

1) Systèmes de congruences:

Application 46: [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?

2) Polynômes et interpolation de Lagrange.

Proposition 47: Soient a_1, \dots, a_r des éléments de \mathbb{K} (\mathbb{R} ou \mathbb{C}) distincts deux-à-deux, des éléments b_1, \dots, b_r de \mathbb{K} . Alors il existe un polynôme $P \in \mathbb{K}[X]$ de degré inférieur à r tel que $\forall k \in \{1, \dots, r\}$
 $P(a_k) = b_k$.

3) Réduction d'endomorphismes:

Théorème 48: [Décomposition des noyaux]

Soit E un \mathbb{K} eu de dimension $n \in \mathbb{N}^*$.

$P = P_1 \dots P_k \in \mathbb{K}[X]$ où les P_i sont premiers entre eux deux-à-deux. Alors

$$\ker(P(f)) = \ker(P_1(f)) \oplus \dots \oplus \ker(P_k(f))$$

Théorème 49: [Décomposition de Dunford] Soit $f \in \mathcal{L}(E)$ tel que son polynôme caractéristique soit scindé sur \mathbb{K} .

Il existe un unique couple d'endomorphismes (d, n) tels que

i) $f = d + n$

ii) d et n commutent

iii) d est diagonalisable et n nilpotent

iv) d et n sont dans $\mathbb{K}[f]$.

4) Extension de corps:

Définition 50: Soit $\mathbb{K} \subset \mathbb{L}$. $\alpha \in \mathbb{L}$ est algébrique si il existe $P \in \mathbb{K}[X]$ tq $P(\alpha) = 0$

Théorème 51: Si $\alpha \in \mathbb{L}$ est algébrique sur \mathbb{K} , il existe un

unique $P \in \mathbb{K}[X]$ unitaire irréductible tel que $P(\alpha) = 0$. C'est le polynôme minimal de α et $[\mathbb{K}(\alpha) : \mathbb{K}] = \deg(P)$.

[Ro] [257]

[Ro] [260]

[Ro] [261]

[Esc]

[Esc]

[Esc] [455]

[Esc] [463]

[X6] [475]

[X6] [195]

[Ro] [246]