Leçon 122 : Anneaux principaux. Exemples et Applications

I) Généralités

[BER] p405 id. principal, A principal... + p459 id. premier, maximal...

II) Arithmétique dans les anneaux.

a) Divisibilité, éléments irréductibles et premiers.

[BER] p515

b) Anneaux principaux

[BER] p524 Bézout, Gauss, Euclide.

c) Anneaux Euclidiens.

[BER] p529 déf, Euclidien => principal. + [FRA-A1] p48 Vinogradov

d) Anneaux Factoriels.

[ULM] p63 généralités + [BER] p622 A[X] factoriel ssi A factoriel
+ ~~p522~~ Z[i√3] non factoriel

III) Applications.

a) Réduction des endomorphismes.

[BER] p941

b) Anneau Z[i]. [PER] p56

c) Théorème Chinois. [BER] p463 DEV1

d) Idéaux premiers de K[X,Y].

[FRA-A1] p61 DEV2

180

Commentaires :

- Leçon facile, facile à faire.
- Faire la leçon : Ouvrir le [BER].

Partie I pour quelques rappels.
Partie II a) généralités de la notion d'arithmétique puis b), c) et d) pour spécifier. (On met bien les implications corps => euclidien => principal => factoriel (cepf) qui justifient leur présence dans la leçon.
Pour la partie d) utiliser plutôt le [BER] (-1 réf)
Partie III) il faut se faire plaisir, a) c'est [BER] engendre l'essentiel lié à la leçon (cf rapport du Jury).
b) ça pourrait être un DEV, cf [PER].
c) Pour le DEV 1 dans [BER], version un peu différente.
d) Pour le DEV 2, [FRA-A1].

DEV1 : Thm Chinois et applications, 73, 74, 76 et 78, [BER] p463.

DEV2 : Idéaux premiers de K[X,Y], 80, [FRA-A1] p61

Références :

[BER] : G. Berhuy : Algèbre, le grand combat 2e édition
[FRA-A1] : FGN : Exercices de maths pour l'agrég - algèbre 1.
[PER] : D. Perrin : Cours d'algèbre 3e édition.
[ULM] : F. Ulmer : Anneaux, corps, résultants.

Leçon 122 : Anneaux principaux. Exemples et Applications.

I) Idéaux et anneaux principaux / Généralités.

[BER] p405

$(A,+,\cdot)$ un anneau commutatif unitaire.

Déf 1 : Un idéal est un $\mathbb{M}$-groupe I de $(A,+)$ absorbant pour $\times$ (i.e. : $\forall a \in A \times I$, $a i \in I$).

Exc 2 : $\{0\}$, A sont des idéaux. Dans $\mathbb{Z}$, $n\mathbb{Z}$ est un idéal $\forall n \in \mathbb{Z}$.

Lemme 3 : $\varphi : A \to B$ un morphisme d'anneau. $I \trianglelefteq B$ alors $\varphi^{-1}(B) \trianglelefteq A$.

Rq 4 : En particulier $\ker(\varphi) \trianglelefteq A$.

Lemme 5 : L'intersection d'une famille d'idéaux de A est un idéal de A.

Déf 6 : $S \subset A$. On définit $(S) = \bigcap_{\substack{I \trianglelefteq A \\ I \supset S}} I$. C'est le plus petit idéal de A contenant S. On l'appelle idéal engendré par S.

Déf 7 : $I \trianglelefteq A$ est dit principal s'il peut être engendré par un élt (i.e. : $\exists a \in A, I = (a)$).

Exc 8 : A est dit principal s'il est intègre et que tout idéal de A est principal.

Exc 8 : $\mathbb{Z}$ est principal

Déf 9 : $I \trianglelefteq A$ est dit premier lorsque $I \neq A$ et $\forall a,b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$.

[BER] p459

Exc 10 : (0) est premier ssi A est intègre.

Déf 11 : $I \trianglelefteq A$ est dit maximal lorsque $I \neq A$ et $\forall J \trianglelefteq A$, $I \subset J \subset A \Rightarrow J = I$ ou $J = A$.

Exc 12 : Pour p premier, $p\mathbb{Z} \trianglelefteq \mathbb{Z}$ est premier et maximal.

Th 13 : (i) $I \trianglelefteq A$ premier ssi A/I est intègre

(ii) $I \trianglelefteq A$ maximal ssi A/I est un corps

En particulier, tout idéal maximal est premier

II) Divisibilité dans les anneaux

a) Divisibilité, éléments irréductibles et premiers

[BER] p515

Déf 14 : A commutatif. $a,b \in A$. On dit que a divise b s'il existe $x \in A$ tq $b = ax$. Ou de manière équivalente, $(b) \subset (a)$. On le note $a \mid b$.

Exc 15 : La divisibilité est relative à A : Dans $\mathbb{Z}$, $2 \nmid 3$ mais dans $\mathbb{Q}$, $3 = 2 \cdot \frac{3}{2}$.

Déf 16 : On dit que $a,b \in A$ sont associés lorsque $a \mid b$ et $b \mid a$, autrement dit $(a) = (b)$.

Lorsque A est intègre, cela revient à dire que $b = au$ avec $u \in A^\times$.

La relation « être associés » est une relation d'équivalence.

Déf 17 : $a,b \in A$ sont premiers entre eux si $\forall d \in A$, $d \mid a$ et $d \mid b \Rightarrow d \in A^\times$

Autrement dit, deux éléments sont premiers entre eux si leurs div. communs sont les éléments inversibles.

Déf 18 : A un anneau. $a,b \in A$. On dit que d est un pgcd de a et b lorsque :

(i) $d \mid a$ et $d \mid b$ et (ii) $\forall c \in a$, $c \mid a$ et $c \mid b \Rightarrow c \mid d$

On dit que m est un ppcm de a et b lorsque :

(i) $a \mid m$ et $b \mid m$ et (ii) $\forall c \in A$, $a \mid c$ et $b \mid c \Rightarrow m \mid c$.

Rq 19 : a et b sont premiers entre eux ssi 1 est un pgcd de a et b.

Déf 20 : $\pi \in A$ est dit irréductible s'il est non nul, non inversible et si pour tous $a,b \in A$, on a : $\pi = ab \Rightarrow a \in A^\times$ ou $b \in A^\times$.

Exc 21 : $n \in \mathbb{Z}$ est irréductible ssi $n = \pm p$ pour p premier.

Sur $\mathbb{Z}[i\sqrt{6}]$, 2 et $1 \pm i\sqrt{3}$ sont irréductibles non associés car $2 \mid 2$.

Rq 22 : K un corps. $P \in K[X]$ irréductible ssi il n'est pas constant et ne peut pas s'écrire comme produit de deux polynômes non constants. C'est la définition usuelle de P irréductible.

Exc 23 : $P \in \mathbb{C}[X]$ irréductible ssi $d^\circ P = 1$; $P \in \mathbb{R}[X]$ irréductible ssi $d^\circ P = 1$ ou $d^\circ P = 2$ et $\Delta < 0$.

Déf 24 : $\pi \in A$ est dit premier s'il est non nul, non inversible et si pour tous $a,b \in A$, $\pi \mid ab \Rightarrow \pi \mid a$ ou $\pi \mid b$.

De manière équivalente π est premier si (π) est premier non nul.

Exc 25 : Sur $\mathbb{Z}[i\sqrt{5}]$, 2 est irréductible mais pas premier : $2 \mid 4 = (1+i\sqrt{5})(1-i\sqrt{5})$ mais $2 \nmid 1 \pm i\sqrt{5}$.

b) Arithmétique des anneaux principaux. A principal

[BER] p524

Prop 26 : $a,b \in A$. Soient $m,d \in A$ tq $(a)+(b) = (d)$ et $(a) \cap (b) = (m)$

Alors d est un pgcd de a et b et m est un ppcm de a et b.

Cor 27 : $a,b \in A$ premiers entre eux ssi a,b étrangers (i.e. : $\exists (u,v) \in A^2$ tq $ua + vb = 1$) (Bézout)

Lemme 28 (Gauss sur les anneaux principaux) : $a,b \in A$ premiers entre eux.

Alors pour tout $c \in A$, $a \mid bc \Rightarrow a \mid c$

Lemme 29 (Euclide sur les anneaux principaux) : Soit $\pi \in A$ irréductible.

Alors, pour tous $a,b \in A$, $\pi \mid ab \Rightarrow \pi \mid a$ ou $\pi \mid b$.

Prop 30 : Tout idéal premier non nul est maximal

Corollaire 31 : $\pi \in A^*$, LASSE :

(i) $A/(\pi)$ est un corps (ii) $A/(\pi)$ est intègre et (iii) π est irréductible

c) Anneaux euclidiens

p529

Déf 32 : Un anneau euclidien est un couple (A,δ) où A est un anneau intègre et $\delta : A^* \to \mathbb{N}$ est une application telle que, pour tout $a \in A$ et tout $b \in A^*$, il existe $q,r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\delta(r) < \delta(b)$.

Exc 33 : $\mathbb{Z}$ pour $|\cdot|$; $K[X]$ pour $d^\circ(\cdot)$

Prop 34 : Tout anneau euclidien est principal.

Rq 35 : Si (A,δ) euclidien, on met en place l'algorithme d'Euclide

Prop 36 : $a,b \in A$ euclidien. Le dernier reste non nul de l'algorithme d'Euclide d est un pgcd de a et b et on a la relation de Bézout : $\exists u,v \in A, ua+vb=d$

Prop 37 : $A[X]$ est principal ssi A est un corps

d) Anneaux Factoriels.

Déf 38 : A est factoriel s'il est intègre si tout élément non nul, non inv. admet une décomposition en produits d'irréductibles unique à ordre et inversibles près.

Thm 39 : A intègre. LASSE : (i) A est factoriel.

(ii)(a) tout $a \in A$ non nul, non inv. possède une décomp. en produit d'irréductibles.

(b) tout élément irréductible de A est premier.

(iii) Tout élément non nul, non inversible dans A est produit d'elts premiers

Déf 40 : A intègre. Un Système représentatifs d'éléments premiers (Snep) d'élts premiers de A tq tt premier de A est associé à un seul élt de Snep. Pour $a \in A$, $v_p(a)$ est la multiplicité de p dans la décomp de a.

Prop 41 : A factoriel. Après avoir fixé Snep. $a \in A^*$ possède une unique décomposition $a = u_a \prod_{p \in Snep} p^{v_p(a)}$, $u_a \in A^\times$, $v_p(a) \in \mathbb{N}$ presque tous nuls.

Ex 42 : Dans $\mathbb{Z}$, un choix standard de Snep est l'ens. des premiers non nuls

Dans $K[X]$, un choix standard de Snep est l'ens. des polynômes irréd.-unitaires

Prop 43 : A factoriel. Snep. $a,b \in A^\times$. Alors :

(i) $a \mid b \iff v_p(a) \leq v_p(b)$ $\forall p \in Snep$;

(ii) $\prod_{p \in Snep} p^{\min\{v_p(a), v_p(b)\}}$ est un pgcd de a et b ;

(iii) $\prod_{p \in Snep} p^{\max\{v_p(a), v_p(b)\}}$ est un ppcm de a et b.

Rq 44 : Dans un anneau factoriel, il existe toujours un pgcd et un ppcm. (d'éléments non nul)

Rq 45 : Les lemmes d'Euclide et de Gauss restent vrai dans A factoriel

Rq 46 : ⚠ Plus de lien avec les idéaux dans A non principal.

Ce qui nous fait perdre la relation de Bézout

Et le (i) est faux ! Par exp, 2 et X premiers entre eux mais non étrangers

Thm 47 : Tout anneau principal est factoriel.

Thm 48 (Gauss) : $A[X]$ factoriel ssi A factoriel. Dans ce cas : Les irréductibles de $A[X]$ sont : (i) les irréductibles de A.

(ii) Les polynômes non constants primitifs et irréductibles dans $K_A[X]$

Ex 49 : $\mathbb{Z}[X_1, X_2, \dots]$ est factoriel

Ex 50 : $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel, $4 = 2 \cdot 2 = (1+i\sqrt{3})(1-i\sqrt{3})$

III) Applications

a) Réduction des endomorphismes.

E un K-ev. $u \in \mathcal{L}(E)$. $P = a_n X^n + \dots + a_1 X + a_0 \in K[X]$ on a : $u^k = u \circ \dots \circ u$ et $u^0 = Id_E$ by : $P(u) = a_n u^n + \dots + a_1 u + a_0 Id_E \in \mathcal{L}(E)$

Déf 51 : Un endomorphisme de E de la forme $P(u)$, $P \in K[X]$ est appelé polynôme d'endomorphisme en u. On note $K[u] = \{P(u) : P \in K[X]\}$

Rq 52 : $K[u]$ est une sous-algèbre commutative de $\mathcal{L}(E)$.

Lemme 53 (de décomposition des noyaux) Soient $P_1, \dots, P_n \in K[X]$ premiers entre eux deux à deux. Pour tout $u \in \mathcal{L}(E)$, on a :

$$Ker((P_1 \dots P_n)(u)) = Ker(P_1(u)) \oplus \dots \oplus Ker(P_n(u))$$

Déf 54 : $u \in E$. L'annulateur de u : $Ann(u) = \{P \in K[X] \mid P(u) = 0\}$.

Lemme 55 : $Ann(u)$ est un idéal de $K[X]$.

Prop 56 : E un K-ev de dim finie. $u \in \mathcal{L}(E)$. $Ann(u)$ est non nul Et il existe un unique polynôme unitaire $\mu_u \in K[X]$ tq $Ann(u) = (\mu_u)$.

Déf 57 : μ_u est appelé pol. minimal de u. Il est caractérisé de manière unique par : (i) μ_u unitaire ; (ii) $\mu_u \neq 0$; (iii) $\forall P \in K[X]$, $P(u) = 0 \Rightarrow \mu_u \mid P$.

On nomme, c'est l'unique pol. unitaire de $K[X]$ tq $\forall P \in K[X]$, $P(u) = 0 \iff \mu_u \mid P$.

Prop 58 : $\dim E = n$, $u \in \mathcal{L}(E)$, alors $\mu_u \mid \chi_u \mid \mu_u^n$.

Rq 59 : Le théorème de Cayley-Hamilton donne $\chi_u \in (\mu_u)$.

Thm 60 : $u \in \mathcal{L}(E)$. LASSE : (i) u diagonalisable ; (ii) $\prod_{\lambda \in Sp(u)} (X - \lambda)$ annule u ; (iii) $\exists P \in Ann(u)$ scindé simple (iv) μ_u scindé simple (v) $\mu_u = \prod_{\lambda \in Sp(u)} (X - \lambda)$.

[ULM] p
[BER] p627
[BER] p522
[BER] p941

[PER] p56

b) $\mathbb{Z}[i]$ et le théorème des deux carrés

On souhaite déterminer quels entiers sont somme de deux carrés.

Déf 61 : On pose $\Sigma := \{n \in \mathbb{N} / n = a^2 + b^2 \ ; \ a, b \in \mathbb{N}\}$.

Ex 62 : $0 = 0^2 + 0^2$; $9 = 3^2 + 0^2$; $5 = 2^2 + 1^2$.

Déf 63 : On appelle $\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss.

Rq 64 : Si p premier est somme de deux carrés, il n'est plus premier dans $\mathbb{Z}[i]$: $5 = (2+i)(2-i)$

Prop 65 : $\mathbb{Z}[i]$ est muni de la conjugaison : $\sigma : z = a+ib \in \mathbb{Z}[i] \longmapsto \bar{z} = a - ib \in \mathbb{Z}[i]$ et de la norme : $N : z = a+ib \in \mathbb{Z}[i] \longmapsto z\bar{z} = a^2 + b^2 \in \mathbb{N}$.
Et N est multiplicative : $N(zz') = N(z)N(z')$.

Prop 66 : $\mathbb{Z}[i]^* = \{\pm 1 \ ; \pm i\}$.

Prop 67 : Σ est stable par multiplication.

Prop 68 : $(\mathbb{Z}[i], N)$ est Euclidien, donc principal.

Thm 69 : p premier. $p \in \Sigma \iff p = 2$ ou $p \equiv 1 \ [4]$.
$\iff p$ n'est pas irréductible dans $\mathbb{Z}[i]$.
$\iff -1 \in (\mathbb{F}_p^*)^2$ [-1 est un carré dans $\mathbb{F}_p^*$]

Thm 70 : $n \in \mathbb{N}^*$, $n \neq 1$. $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$.
Alors $n \in \Sigma \iff v_p(n)$ pair pour $p \equiv 3 \ [4]$.

[BER] p463

c) Théorème chinois.

Déf 71 : $a, b \triangleleft A$. a, b sont dit comaximaux lorsque $a + b = A$.

Lemme 72 : $a_1, \dots, a_{n+1} \triangleleft A$ deux à deux comaximaux, alors $a_1 \dots a_n$ et a_{n+1} sont comaximaux.

Prop 73 : $a_1, \dots, a_n \triangleleft A$ deux à deux comaximaux. Pour tous $x_1, \dots, x_n \in A$, il existe $x \in A$ tq $x \equiv x_i \ [a_i]$ $\forall i \in [\![1, n]\!]$.

Thm 74 : A principal. $a_1, \dots, a_m \in A$ deux à deux étrangers.
Pour $i \in [\![1, n]\!]$, on pose $\pi_i : A \to A/(a_i)$.
Alors le morphisme $\varphi : A \to A/(a_1) \times \dots \times A/(a_m)$, $x \longmapsto ([x]_1, \dots, [x]_m)$ est surjectif de noyau $(a_1 \dots a_m)$. Ce qui induit : $A/(a_1 \dots a_m) \simeq A/(a_1) \times \dots \times A/(a_m)$.

DÉV 1.A

[On considère A principal]

Déf 75 On pose $\varphi : A/(a_1 \dots a_m) \xrightarrow{\sim} A/(a_1) \times \dots \times A/(a_m)$ de (73).
$\bar{x} \longmapsto ([x]_1, \dots, [x]_m)$

Prop 76 : On pose $\bar{e}_i = \varphi^{-1}(\varepsilon_i)$ avec $\varepsilon_i = (\pi_1(0), \dots, \pi_{i-1}(0), \pi_i(1), \pi_{i+1}(0), \dots, \pi_m(0))$
Et on a : $\varphi^{-1} : A/(a_1) \times \dots \times A/(a_m) \xrightarrow{\sim} A/(a_1 \dots a_m)$
$([x_1], \dots, [x_m]) \longmapsto \sum_{i=1}^{m} e_i x_i$. DEV 1.B

Rq 77 : Pour calculer explicitement φ^{-1}, on détermine pour $i \in [\![1, n]\!]$ une solution du système de congruence $x \equiv \delta_{ij} \ [a_i]$, $j \in [\![1, m]\!]$.
Ce qui équivaut, par principalité de A, à $e_i \equiv 1 \ [a_i]$ et $e_i \equiv 0 \ [\prod_{j \neq i} a_j]$

DÉV 1.C

Appli 78 : L'inverse de $\varphi : \mathbb{Z}/84\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ est :
$\varphi^{-1} : \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/84\mathbb{Z}$
$(\widehat{x_1}, \widehat{x_2}, \widehat{x_3}) \longmapsto \overline{28x_1 + 21x_2 + 36x_3}$

Appli 79 : L'inv. de $\varphi : \mathbb{R}[X]/(X^4 + X^2) \xrightarrow{\sim} \mathbb{R}[X]/(X^2) \times \mathbb{R}[X]/(X^2+1)$
$\overline{P} \longmapsto (\hat{P}, \tilde{P})$
est $\varphi^{-1} : (\hat{P}, \tilde{Q}) \longmapsto \overline{(X^2+1)P - X^2 Q}$

DÉV 2

d) Étude des idéaux premiers de $K[X, Y]$ [FRA-AI] p61

K un corps infini

Thm 80 : Les idéaux premiers de $K[X, Y]$ sont les idéaux :
- Principaux : de la forme (P) avec P irréductible ou (0)
- Non principaux de la forme $(P(X), R(X, Y))$ avec $P(X) \in K[X, Y]$ irréductible et $R(X, Y) \in K[X, Y]$ tel que $\overline{R(X,Y)}$ soit irréductible dans l'anneau $(K[X]/(P))[Y]$.