122. Anneaux principaux. Applications

Tous les anneaux seront considérés comme commutatifs.
$(A,+,\cdot)$ désigne un anneau.

I. Idéaux, anneaux factoriels

1) Idéaux

Déf. 1 : $I \subset A$ est appelé un idéal de A si :
i) $(I,+)$ est un groupe
ii) $\forall a \in A, \forall x \in I, \quad ax \in I$

Si $a \in A$, on notera $(a) = \{ba, b \in A\}$ l'idéal engendré par a. Un tel idéal est dit principal.

Ex 2 : . $\{0\}$ et A sont des idéaux de A
. Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$
. Si K est un corps, ses seuls idéaux sont $\{0\}$ et K.

Th. 3 : (projection canonique)
Si $I \subset A$ est un idéal, il existe une unique structure d'anneau sur A/I telle que $\pi : \begin{array}{l} A \longrightarrow A/I \\ a \longmapsto a \bmod I \end{array}$ soit un morphisme d'anneaux.

[Per] 43

Déf. 4 : Un idéal $I \subset A$ est dit premier si : $I \neq A$ et pour tout $(a,b) \in A^2$, $ab \in I \Rightarrow a \in I$ ou $b \in I$.
$a \in A$ est dit premier si (a) est premier

Ex 5 : Les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et $p\mathbb{Z}$, p nombre premier

Prop. 6 : $I \subset A$ idéal premier SSI A/I est intègre

Déf. 7 : Un idéal $I \subset A$ est dit maximal si : $I \neq A$ et pour tout idéal $J \subset A$, $I \subset J \Rightarrow J = I$ ou $J = A$.

Prop. 8 : $I \subset A$ idéal maximal SSI A/I est un corps.

Cor 9 : I maximal $\Rightarrow$ I premier

Ex 10 : Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$, p nombre premier

Tous les anneaux sont désormais intègres

2) Arithmétique dans un anneau intègre

[Per] 46

Déf. 11 : . $a \in A$ est dit inversible si il existe $b \in A$ tel que $ab = 1$.
On note $A^\times$ l'ensemble des inversibles de A.
. $a, b \in A$. On dit que a divise b, noté $a|b$ s'il existe $c \in A$ tel que $b = ac$.

Ex. 12 : . $\mathbb{Z}^\times = \{\pm 1\}$.
. $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{k} \in \mathbb{Z}/n\mathbb{Z}, k \wedge n = 1\}$ (exemple non intègre...)

Prop. 12 : $a|b \iff (b) \subset (a)$

Déf./Prop 13 : Soient $a, b \in A$. On dit que a et b sont associés, noté $a\mathcal{R}b$ si : $a|b$ et $b|a \iff (a) = (b) \iff \exists u \in A^\times \,/\, a = ub$ 46
$\mathcal{R}$ est une relation d'équivalence.

Déf. 14 : $p \in A$ est dit irréductible si $p \notin A^\times$ et $p = ab \Rightarrow a \in A^\times$ ou $b \in A^\times$
On notera $\mathcal{P}$ un ensemble de représentants des classes des irréductibles de A pour la relation $\mathcal{R}$.

Ex 15 : Les irréductibles dans $\mathbb{Z}$ sont les nombres premiers.

Déf. 16 : $a, b \in A$ sont dits premiers entre eux, noté $a \wedge b = 1$ si :
$\forall d \in A$, $d|a$ et $d|b \Rightarrow d \in A^\times$

3) Anneaux factoriels

Déf. 17 : Un anneau intègre A est dit factoriel si :
(E) $\forall a \in A, a \neq 0, \quad a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ où $u \in A^\times$, $v_p(a) \in \mathbb{N}$ et les $v_p(a)$ sont presque tous nuls. 47
(U) Cette écriture est unique.

Prop. 18 : Dans A factoriel, $a|b \iff \forall p \in \mathcal{P}, v_p(a) \leq v_p(b)$

Ex 19 : $\mathbb{Z}$ est factoriel

Déf. 20 : Soient $a, b \in A$ anneau factoriel.
"Le" pgcd de a et b, est $a \wedge b = \text{pgcd}(a,b) = \prod_{p \in \mathcal{P}} p^{\inf(v_p(a), v_p(b))}$ 49

"Le" ppcm de a et b est $a \vee b = \text{ppcm}(a,b) = \prod_{p \in \mathcal{P}} p^{\sup(v_p(a), v_p(b))}$

Rq (21) : . $a \wedge b$ et $a \vee b$ sont définies modulo $A^\times$
. $(a) \cap (b) = (a \vee b)$, mais on n'a pas nécessairement $(a)+(b) = (a \wedge b)$.
En admettant que $\mathbb{Z}[X]$ est factoriel, $\text{pgcd}(2, X) = 1$, et
$(2)+(X) = (2,X) \neq (1) = \mathbb{Z}[X]$ car $3 \notin (2,X)$.

Prop. (22) : Soit A anneau intègre vérifiant (E). Sont équivalentes :
i) A est factoriel
ii) (Euclide) si p irréductible et $p \mid ab$, alors $p \mid a$ ou $p \mid b$
iii) p irréductible $\Leftrightarrow$ p premier et $p \neq 0$.
iv) (Gauss) si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

II. Anneaux principaux

1) Définition, propriétés et premiers exemples

Déf. (23) : Un anneau A est dit principal s'il est intègre et si tout idéal de A est principal.

Ex. (24) : $\mathbb{Z}$ est principal

Prop. (25) : Un anneau principal est factoriel

Rq (26) : La réciproque est fausse ! (voir Rq (27))

Th. (27) : (Bezout)
Soit A un anneau principal, $a, b \in A \setminus \{0\}$ et $d = \text{pgcd}(a,b)$.
Alors : $(a)+(b) = (d)$, i.e. $\exists\, \lambda, \mu \in A \,/\, \lambda a + \mu b = d$

Coro (28) : Sous les mêmes hypothèses,
$a \wedge b = 1 \Leftrightarrow \exists\, \lambda, \mu \in A \,/\, \lambda a + \mu b = 1$

Prop. (29) : Les idéaux premiers de A principal sont $\{0\}$ et (p) où p est irréductible. $A/(p)$ est alors un corps.

Th. (30) : (des restes chinois)
Soit A anneau principal, $a, b \in A$ tels que $a \wedge b = 1$. Alors
$\varphi : A/(ab) \longrightarrow A/(a) \times A/(b)$ est un isomorphisme d'anneaux
$x \bmod ab \longmapsto (x \bmod a, x \bmod b)$

Déf. (31) : Un anneau intègre A est dit euclidien si :
$\exists\, v : A \setminus \{0\} \to \mathbb{N} \,/\, \forall a, b \in A \setminus \{0\}, \exists\, q, r \in A,\ a = bq + r$ et $r = 0$ ou $v(r) < v(b)$.

Ex (32) : $(\mathbb{Z}, |\cdot|)$ est euclidien

Prop. (33) : A euclidien $\Longrightarrow$ A principal

Rq (34) : La réciproque est fausse ! $\left(\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]\right)$

2) Anneaux de polynômes

Lemme (35) : (division euclidienne généralisée)
Soit $S, P \in A[X]$, $P \neq 0$ et de coefficient dominant inversible dans A.
Alors : $\exists\, Q, R \in A[X] \,/\, S = PQ + R$ où ($R = 0$ ou $\deg R < \deg P$).

Prop. (36) : $A[X]$ principal $\Leftrightarrow$ A est un corps $\Leftrightarrow$ $A[X]$ euclidien

Rq (37) : A principal $\not\Leftrightarrow$ $A[X]$ principal $(\mathbb{Z}[X])$

Déf. (38) : Soit A factoriel, $P = a_n X^n + \dots + a_0 \in A[X]$. Le contenu de P est $c(P) = \text{pgcd}(a_0, \dots, a_n)$ (défini modulo $A^\times$).
P est dit primitif si $c(P) = 1$.

On suppose A factoriel jusqu'à la fin de II. 2), et on note $K = \text{Fr}(A)$.

Lemme (39) : (Gauss).
$P, Q \in A[X]$. $c(PQ) = c(P)c(Q)$.

Prop. (40) : Les polynômes $P \in A[X]$ irréductibles dans $A[X]$ sont :
i) Les polynômes constants $p \in A$, p irréductible dans A
ii) Les polynômes P de degré ≥ 1, primitifs et irréductibles dans $K[X]$

9 18 [pa] 49 ~53 50 53+ 50 51 AVP1

76 DVP 1 **Th. (41)** : (*critère d'Eisenstein*)

Soit $P = a_n X^n + \dots + a_0 \in A[X]$, $n \geq 2$ et $p \in A$ irréductible.

Si : i) $p \nmid a_n$

ii) $\forall\, 0 \leq i \leq n-1$, $p \mid a_i$

iii) $p^2 \nmid a_0$

Alors P est irréductible dans $K[X]$ (et donc dans $A[X]$ si $c(P) = 1$)

Appli. (42) : . il existe des polynômes irréductibles de tout degré dans $\mathbb{Q}[X]$.

. si p est premier, $\Phi_p = X^{p-1} + \dots + X + 1$ est irréductible dans $\mathbb{Z}[X]$.

51 **Th. (43)** : Si A est factoriel, alors $A[X]$ est factoriel.

III. Applications

1) Théorème des restes chinois

[Ber] 469 **Exercice (44)** : Résoudre le système de congruences
$$\begin{cases} x \equiv 1 \ [3] \\ x \equiv 2 \ [4] \\ x \equiv -1 \ [7] \end{cases}$$

[Beck] 244 **Th. (45)** : (*algorithme de Berlekamp*)

Soit $q = p^s$, p premier et $s \geq 1$, $P \in \mathbb{F}_q[X]$ de degré $n \geq 1$ sans facteurs carré. Alors, on peut déterminer $V \in \mathbb{F}_q[X]$ tel que :

i) V est non constant modulo P

ii) $P = \prod_{\alpha \in \mathbb{F}_q} \operatorname{pgcd}(P, V - \alpha)$ $(*)$

iii) si P n'est pas irréductible, au moins deux des facteurs du produit précédent sont non triviaux

Rq (46) : L'algorithme de Berlekamp permet de déterminer la décomposition en facteurs irréductibles d'un polynôme dans un corps fini.

Exercice (47) : p premier > 2. Appliquer et discuter l'algorithme de Berlekamp à $P = X^2 - a$, où $a \in \mathbb{F}_p \setminus \{0\}$.

2) Algèbre linéaire

Cadre : K corps, E un K-ev de dimension finie $n \geq 1$, $u \in \mathcal{L}(E)$, $u \neq 0$. [Ber]

Prop. (48) : $\varphi : K[X] \to \mathcal{L}(E)$, $P \mapsto P(u)$ est un morphisme de K-algèbres.

Il existe un unique $\mu_u \in K[X]$ unitaire irréductible tel que $\operatorname{Ker} \varphi = (\mu_u)$. 942

Rq (49) : ⚠ dimension infinie ! On peut avoir $u \neq 0_{\mathcal{L}(E)}$ et $\mu_u = 0_{K[X]}$. E1 999

Th. (50) : (*lemme des noyaux*)

Soient $P, P_1, P_2 \in K[X]$ tels que $P = P_1 P_2$ et $P_1 \wedge P_2 = 1$. 943

On définit $F = \operatorname{Ker} P(u)$, $F_1 = \operatorname{Ker} P_1(u)$ et $F_2 = \operatorname{Ker} P_2(u)$ des sev de E.

Alors, $F = F_1 \oplus F_2$

De plus, le projecteur de F sur F_1 (resp. F_2) parallèlement à F_2 (resp. F_1) est un polynôme en u.

Appli. (51) : u est diagonalisable $\iff$ u annule un polynôme scindé à racines simples

Appli. (52) : (*décomposition de Dunford*)

Soit $u \in \mathcal{L}(E)$ tel que son polynôme caractéristique χ_u soit scindé.

Alors, il existe $\delta, \nu \in \mathcal{L}(E)$ tels que 968

i) $u = \delta + \nu$

ii) δ et ν commutent

iii) δ est diagonalisable et ν est nilpotent.

Exercice (53) : Soit $\lambda \in \mathbb{R}^*$, $A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. Calculer e^{tA}, $t \in \mathbb{R}$ et en déduire le portrait de phase de $Y' = AY$.

Références :

- [Per] Perrin, Cours d'algèbre
- [Beck] Beck, Malick, Peyré - Objectif agrégation
- [Ber] Berhuy, Algèbre : le grand combat (2^e édition)