122

Anneaux principaux. Applications

Soit A un anneau commutatif, unitaire, intègre.
Soit K un corps.

I - Propriétés fondamentales des anneaux principaux

a.) Anneaux principaux

Définition 1: Soit $I \subset A$ un idéal de A.
- I est premier si $I \subsetneq A$ et $\forall a,b \in I$, $ab \in I \Rightarrow a \in I$ ou $b \in I$
- I est maximal si $I \subsetneq A$ et I est maximal pour l'inclusion : si $J \subsetneq A$ est un idéal et $I \subset J$, alors $I = J$.
- I est principal s'il existe $x \in A$ tel que $I = (x)$.

Proposition 2:
- I est premier $\Leftrightarrow$ A/I est intègre
- I est maximal $\Leftrightarrow$ A/I est un corps

Corollaire 3: I est maximal $\Rightarrow$ I est premier

Exemple 4: Les idéaux premiers de $\mathbb{Z}$ sont $n\mathbb{Z}$ pour $n=0$ ou n premier. Ses idéaux maximaux sont $n\mathbb{Z}$ pour n premier.

Définition 5: $x \in A$ est irréductible si $x \notin A^\times$ et si $x = ab$, alors $a \in A^\times$ ou $b \in A^\times$
x est premier si $x \neq 0$, $x \notin A^\times$ et si $x | ab$, $x | a$ ou $x | b$

Proposition 6:
$$\begin{cases} (x) \text{ maximal} \Rightarrow x \text{ irréductible} \\ x \text{ est premier} \Rightarrow x \text{ est irréductible} \\ x \text{ est premier} \Leftrightarrow (x) \text{ est premier} \end{cases}$$

Exemple 7:
- 2 est irréductible dans $\mathbb{Z}[i\sqrt{3}]$ mais 2 n'est pas premier : $2 | 4 = (1+i\sqrt{3})(1-i\sqrt{3})$ et $2 \nmid (1 \pm i\sqrt{3})$
- Tout $p \in \mathbb{Z}$ premier est un élément premier.

Définition 8: A est principal si tout idéal de A est principal.

Exemple 9:
- $\mathbb{Z}$ est principal, $K[X]$ aussi pour K corps.
- $K[X,Y]$ n'est pas principal car l'idéal (X,Y) n'est pas principal, pourtant $(X,Y) \subsetneq K[X,Y]$

Définition 10: Pour $a,b \in A$, d est un pgcd de a et b si
$$\begin{cases} d | a \text{ et } d | b \\ \forall c \in A \text{ tq. } c|a \text{ et } c|b,\ c|d \end{cases}$$
$m \in A$ est un ppcm de a et b si
- $a|m$ et $b|m$
- $\forall c \in A$ tq $a|c$ et $b|c$, $m|c$

Exemple 11: Dans $\mathbb{Z}$, 2 est un pgcd de 4 et 6

Définition 12: a et b sont premiers entre eux si $(d|a$ et $d|b) \Rightarrow d \in A^\times$

Lemme 13: Lorsqu'ils existent, le pgcd et le ppcm sont uniques à association près

Proposition 14: Si A est principal et $a, b \in A$
- $(a) + (b) = (d)$ où $d \in A$
- $(a) \cap (b) = (m)$ où $m \in A$.

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

Corollaire 15: Il existe alors $\lambda, \mu \in A$ tq. $\lambda a + \mu b = d$

Corollaire 16: (Bezout) Si A est principal et $a, b \in A$, a et b sont premiers entre eux ssi il existe $\lambda, \mu \in A$ tq $\lambda a + \mu b = 1$

Lemme 17: (Gauss) Si A est principal et $a, b \in A$ sont premiers entre eux alors pour $c \in A$, $a | bc \Rightarrow a | c$

Exemple 18: Dans $\mathbb{R}[X]$, $X-1 | (X+1)(X^2-2X+1)$ et $X-1$ et $X+1$ sont premiers entre eux. Donc $X-1 | X^2-2X+1$
Le cas $2 \in \mathbb{Z}[i\sqrt{3}]$ de l'exm. 7 est toujours un contre-exemple.

Théorème 19: (Chinois) Si A est principal, $a_1, \dots, a_n \in A$ deux à deux premiers entre eux et $\pi_i : \begin{cases} A \to A/(a_i) \\ x \mapsto [x]_i \end{cases}$ est la projection canonique, alors $f : \begin{cases} A \to A/(a_1) \times \dots \times A/(a_n) \\ x \mapsto ([x]_1, \dots, [x]_n) \end{cases}$ est un morphisme surjectif, de noyau $(a_1 \cdots a_n)$

Ainsi $A/(a_1 \cdots a_n) \simeq A/(a_1) \times \dots \times A/(a_n)$

Exemple 20: $\mathbb{Z}/(2^2 \times 3 \times 5)\mathbb{Z} \simeq \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Lemme 21: Soit $\pi \in A$ irréductible. Alors (π) est maximal pour l'inclusion parmi les idéaux propres principaux de A. (La réciproque est vraie). En particulier, si A principal, (π) est maximal et π est premier.

Rq 22: Dans A principal, irréductible $\Leftrightarrow$ premier

Lemme 23: A principal, π irréductible. (Euclide)
Si $\pi | ab$, $\pi | a$ ou $\pi | b$

Proposition 24: Si A principal, I idéal non nul, alors
- I maximal $\Leftrightarrow$ I premier.

Corollaire 25: Si A principal et $\pi \in A \setminus \{0\}$, il y a équivalence
- $A/(\pi)$ est un corps
- $A/(\pi)$ est intègre
- π est irréductible.

Corollaire 26: Si A principal, $A[X]$ principal $\Leftrightarrow$ A est un corps

b.) Anneaux factoriel

Définition 27: $P \subset A$ est un système de représentants d'irréductibles si
- $\forall p \in P$, p est irréductible
- $\forall q \in A$ irréductible, $\exists! p \in P$ tel que p et q sont associés.

On fixe $P \subset A$ un tel système.

Définition 28: A est factoriel s'il vérifie
(E) $\forall a \in A \setminus \{0\}$, a s'écrit $a = u \prod_{p \in P} p^{v_p(a)}$ avec $u \in A^\times$ et $(v_p(a))_{p \in P}$ une suite presque nulle d'entiers
(U) cette écriture est unique.

Exemple 29:
$$\begin{cases} K \text{ corps est factoriel} \\ K[X,Y] \text{ est factoriel,} \\ \mathbb{Z}, K[X] \text{ sont factoriels} \end{cases}$$

Remarque 30: Le corollaire 16 est faux en général dans un anneau factoriel : Dans $K[X,Y]$, X et Y sont premier entre eux, mais $1 \notin (X,Y)$

Théorème 31: A factoriel => $A[X]$ factoriel

Corollaire 32: A factoriel => $A[X_1,\dots,X_n]$ factoriel et encore $A[X_1,\dots]$ factoriel

Proposition 33: Soit A vérifiant (E). Alors

- A vérifie (U)

$\Updownarrow$

- $p\in A$ irréductible $\Leftrightarrow$ p premier

$\Updownarrow$

- $a|bc$ et a et b premiers entre eux $\Rightarrow a|c$

Corollaire 34: A principal => A factoriel

Remarque 35: $K[X,Y]$ est factoriel d'après le corollaire 3_, mais n'est pas principal. Donc la réciproque est fausse.

Lemme 36: Si A est factoriel, $a|b \Leftrightarrow \forall p\in P, v_p(a)\leq v_p(b)$

Proposition 37: Si A est factoriel, et $a,b\in A$, alors a et b admettent un pgcd et un ppcm.

De plus, $\mathrm{pgcd}(a,b)=\prod_{p\in P} p^{\min(v_p(a),v_p(b))}$

$\mathrm{ppcm}(a,b)=\prod_{p\in P} p^{\max(v_p(a),v_p(b))}$

à multiplication par un inversible près.

Proposition 38: Cela coïncide avec le pgcd et ppcm dans les anneaux principaux.

Exemple 39: $\mathrm{pgcd}(2^2\times 3\times 17, 2\times 3\times 11)=2\times 3=6$ dans $\mathbb{Z}$ et $\mathrm{ppcm}(2^2\times 3\times 17, 2\times 3\times 11)=2^2\times 3\times 11\times 17$

c.) Anneaux euclidiens

Définition 40: A est euclidien s'il est muni d'une division euclidienne, ie il existe $\delta: A\setminus\{0\}\to\mathbb{N}$ tel que pour $a\in A$ et $b\in A\setminus\{0\}$, il existe $q,r\in A$ tels que $a=qb+r$ et $r=0$ ou $\delta(r)<\delta(b)$.

Remarque 41: Le couple (q,r) n'est pas forcément unique. En effet, dans $\mathbb{Z}$, avec $\delta=|.|$, $5=(-2)\times(-2)+1$ mais aussi $5=(-2)\times(-3)+(-1)$

Proposition 42: A euclidien => A principal

Exemple 43:
- $K[X,Y]$ n'est pas principal donc n'est pas euclidien.
- $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{2}]$, $\mathbb{Z}[j]$ sont euclidiens.

Remarque 44: A principal $\not\Rightarrow$ A euclidien

En effet $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal mais pas euclidien.

Lemme 45: Soit $P\in A[X]\setminus\{0\}$ de coefficient dominant inversible. Alors pour $F\in A[X]$, il existe $Q,R\in A[X]$ tels que $F=QP+R$ et $R=0$ ou $\deg R<\deg P$

Corollaire 46: $K[X]$ est euclidien ($\delta=\deg$)

Remarque 47: Avec le corollaire 26, si A principal $A[X]$ euclidien $\Leftrightarrow$ A est un corps.

Proposition 48: (Euclide étendu) Si (A,δ) est euclidien, il existe un algorithme qui prend en entrée $a,b\in A\setminus\{0\}$ et qui renvoie d,u,v tels que $\begin{cases}\mathrm{pgcd}(a,b)=d \text{ à association près}\\ ua+vb=d\end{cases}$

II - Applications en arithmétique

a) L'anneau $\mathbb{Z}[i]$

Définition 49: $\mathbb{Z}[i]:=\{a+ib \mid a,b\in\mathbb{Z}\}$ est l'anneau des entiers de Gauss.

Proposition 50: $\mathbb{Z}[i]$ est euclidien pour $\delta=N$ où $N(a+ib)=a^2+b^2=(a+ib)\overline{(a+ib)}$

Remarque 51: N est multiplicative

Proposition 52: $\mathbb{Z}[i]^\times=\{\pm 1,\pm i\}$ et les irréductibles de $\mathbb{Z}[i]$ sont, à association près,
- $p\in\mathbb{N}$ premiers tels que $p\equiv 3\,[4]$
- $a+ib$, tels que a^2+b^2 premier dans $\mathbb{Z}$.

Théorème 53: $n\in\mathbb{N}\setminus\{0\}$ est une somme de carrés d'entiers $\Leftrightarrow$ $\forall p$ premier avec $p\equiv 3[4]$, $v_p(n)$ pair

Exemple 54: $45=3^2\times 5=3^2+6^2$

b) Autres anneaux particuliers en arithmétique

Proposition 55: $\mathbb{Z}[\frac{1+i\sqrt{7}}{2}]$ est euclidien (donc principal)

DEV1

Application 56: (Ramanujan-Nagell) Les solutions entières de $x^2+7=2^n$ sont $(x,n)=(1,3),(3,4),(5,5),(11,7)$ et $(181,15)$.

Proposition 57: $\mathbb{Z}[j]$ est euclidien.

Application 58: (Fermat, n=3) L'équation $x^3+y^3=z^3$ n'a aucune solution non triviale dans $\mathbb{Z}^3$.

III - Applications en algèbre linéaire

a.) L'anneau $K[X]$ et les $K[X]$-modules

Remarque 59: On rappelle que $K[X]$ est un anneau euclidien (donc principal, donc factoriel)

Corollaire 60: Soit E un K-espace vectoriel de dimension finie. Soit $u\in\mathcal{L}(E)$. Alors il existe un unique polynôme unitaire, noté π_u, qui divise tout polynôme annulateur de u, dans $K[X]$.

Corollaire 61: (Lemme des noyaux) Soient $P_1,\dots,P_r \in K[X]$ premiers entre eux deux à deux, et $u \in \mathcal{L}(E)$.
Alors $\operatorname{Ker}(P_1\cdots P_r(u)) = \operatorname{Ker}(P_1(u)) \oplus \cdots \oplus \operatorname{Ker}(P_r(u))$

Définition 62: Un A-module est un groupe abélien M muni d'un morphisme $\varphi : A \to \operatorname{End}_{gr}(M)$.

Remarque 63: Si A est un corps, M est un A-e.v.

Exemple 64: · Les $\mathbb{Z}$-modules sont exactement les groupes abéliens.
· Les $K[X]$-modules sont les K-e.v. munis d'un endomorphisme.

Définition 65: Un sous-module d'un A-module M est un sous-groupe de M, stable par chaque $\varphi(a)$, $a\in A$
· Pour $N\subset M$, l'annulateur de N est l'idéal $\operatorname{Ann}_A(N) = \{a\in A \mid \forall x\in N, \varphi(a)(x)=0\}$
· M est un module cyclique s'il est engendré par x d'annulateur non nul.

Exemple 66: · Les $\mathbb{Z}$-modules cycliques sont les groupes cycliques.

Proposition 67: · Soit E de dimension finie et soit $u\in\mathcal{L}(E)$. Alors l'annulateur du $K[X]$-module (E,u) est (π_u).
· De plus (E,u) est cyclique ssi u est un endomorphisme cyclique.

b.) Forme normale de Smith et réduction de Frobenius

DEV2

Soit A un anneau principal.

Théorème 68: Soit $U \in \mathcal{M}_{m,n}(A)$. Alors il existe $(d_1,\dots,d_s)$ une famille de A tels que $d_1|\cdots|d_s$ et tels que U soit équivalente à la matrice

$$D = \left(\begin{array}{ccc|c} d_s & & & \\ & \ddots & & 0 \\ & & d_1 & \\ \hline & 0 & & 0 \end{array}\right)$$

De plus, si U est équivalente à $D' = \left(\begin{array}{ccc|c} d'_t & & & \\ & \ddots & & 0 \\ & & d'_1 & \\ \hline & 0 & & 0 \end{array}\right)$

alors $s=t$ et pour tout i, d_i est associé à d'_i.

Exemple 69: Pour $A=\mathbb{Z}$ et $C = \begin{pmatrix} 10 & 14 \\ 6 & 7 \end{pmatrix}$, alors $U = \begin{pmatrix} 1 & 0 \\ 0 & -14 \end{pmatrix}$

Théorème 70: (de la base adaptée) Soit M un A-module libre de rang m. Soit N un sous-module.
Alors il existe une base $(e_1,\dots,e_m)$ de M, un entier $r\geq 0$ et $a_1,\dots,a_r\in A$ tels que $a_1|\cdots|a_r$ et $(a_1e_1,\dots,a_re_r)$ soit une base de N.
En particulier, N est libre de rang $r\leq m$ et r et les idéaux $(a_1),\dots,(a_r)$ sont uniques.

Exemple 71: Considérons le $\mathbb{Z}$-module $M=\mathbb{Z}^3$ de rang 3. Soit N le sous-module engendré par $\begin{pmatrix} 4 \\ -2 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 2 \\ -2 \\ 2 \end{pmatrix}$ et $\begin{pmatrix} -3 \\ 0 \\ 3 \end{pmatrix}$. Alors $m=3$, $r=2$, et on prend $a_1 = \begin{pmatrix} 1 \\ -2 \\ 3 \end{pmatrix}$, $a_2 = \begin{pmatrix} 0 \\ 1 \\ -2 \end{pmatrix}$ et $a_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Ainsi $(a_1, 2a_2)$ est une base de N.

Remarque 72: Tout sous-groupe de $\mathbb{Z}^m$ est isomorphe à $\mathbb{Z}^r$ pour un $r\leq m$.

Théorème 73: (Structure des modules de type fini sur un anneau principal) Soit M un A-module non nul de type fini.
Alors il existe $r,s\geq 0$, $a_1,\dots,a_s\in A\setminus\{0\}$ et $M_1,\dots,M_s, L$ des sous-modules tels que
- $a_1|\cdots|a_s$
- $M_1,\dots,M_s$ sont non nuls, cycliques et $\forall i$, $\operatorname{Ann}_A(M_i)=(a_i)$
- L est libre de rang r
- $M = M_1\oplus\cdots\oplus M_s\oplus L$

L'entier r et $(a_1),\dots,(a_s)$ caractérise M à isomorphisme près. De plus $r = \operatorname{rg}_A(M)$.

Corollaire 74: (réduction de Frobenius) Soit E un K-ev de dimension finie, et soit $u\in\mathcal{L}(E)$.
Alors il existe une décomposition de E en somme directe de s.e.v. stables par u, non nuls $E = E_1\oplus\cdots\oplus E_r$ et des polynômes unitaires non constants $\chi_1,\dots,\chi_r$ tels que $\chi_1|\cdots|\chi_r$ et $\forall i$, $u|_{E_i}$ est cyclique de polynôme minimal χ_i.
De plus $(\chi_1,\dots,\chi_r)$ sont les invariants de similitude.

Corollaire 75: Soit G un groupe abélien de type fini. Alors $\exists r,s\geq 0$, $\exists n_1,\dots,n_s\geq 2$ tq. $n_1|\cdots|n_s$ et $G\simeq \mathbb{Z}/n_1\mathbb{Z}\times\cdots\times\mathbb{Z}/n_s\mathbb{Z}\times\mathbb{Z}^r$
De plus $r, n_1,\dots,n_s$ sont uniques et caractérise la classe d'isomorphisme de G.

Pour A anneau intègre :

$$\begin{array}{ccccc}
 & & A \text{ euclidien} & \Longrightarrow & \text{Algorithme d'Euclide étendu} \\
 & & \Downarrow & & \Downarrow \\
 & & A \text{ principal} & \Longrightarrow & A \text{ de Bézout} \\
 & & \Downarrow & & \\
A[X] \text{ factoriel} & \Longleftarrow & A \text{ factoriel} & \Longrightarrow & \text{Lemmes de Gauss et Euclide} \\
 & & \Downarrow & & \\
 & & \text{Les ppcm existent dans } A & & \\
 & & \Downarrow & & \\
 & & \text{Les pgcd existent dans } A & &
\end{array}$$

Bibliographie.

Perrin — Cours d'Algèbre

Berhuy — Algèbre, le grand combat

Berhuy — Modules : théorie, pratique...

Boyer — Petit compagnon des nombres (DVP 1)

Duverney — Théorie des nombres

Peyré — Objectif Agrégation (DVP 2)