122

Anneaux principaux. Exemples et applications.

12/09/17 réf: F. Ulmer

On considère un domaine d'intégrité A et K un corps

I - Différentes structures sur les anneaux.

(a) Rappels sur les idéaux

def ①: un idéal principal est un idéal engendré par un seul élément.

Exple ②: • les idéaux de $\mathbb{Z}$ sont ceux de la forme $n\mathbb{Z}$ où $n \in \mathbb{Z}$
• $(2, X)$ est un idéal de $\mathbb{Z}[X]$, qui n'est principal

def ③: un idéal I de A est dit premier si l'idéal est propre et si : $\forall a,b \in A$ tq $ab \in I \Rightarrow \left| \begin{array}{l} a \in I \\ \text{ou} \\ b \in I \end{array} \right.$

Exple ④: avec $A = \mathbb{Z}$, les idéaux premiers sont exactement l'idéal nul et les idéaux $n\mathbb{Z}$ avec n premier.

prop ⑤: I est premier ssi A/I est intègre

def ⑥: un idéal I de A est dit maximal s'il est propre et s'il est maximal pour l'inclusion:
Pour tout idéal J de A tq $I \subsetneq J \subset A \Rightarrow J = A$.

prop ⑦: I est maximal ssi A/I est un corps.

prop: ⑧ tout idéal premier est maximal.

Exple ⑨: les idéaux premiers de $K[X,Y]$ sont exactement
• l'idéal nul
• les idéaux de la forme (P) où P irréductible.
• les idéaux maximaux : de la forme $(X-a, Y-b)$ où $a,b \in K^2$

(b) Anneaux principaux

def: ⑩: A est dit principal si tous ses idéaux sont principaux.

Exple ⑪: • $\mathbb{Z}$ et $K[X]$ sont principaux
• $\mathbb{Z}[X]$ ne l'est pas.

App ⑫: (polynome minimal) pour $f \in \mathcal{L}(E)$, l'idéal $I = \{P \in K[X] : P(f) = 0\} \subset K[X]$ est engendré par un "unique" polynome, le polynome minimal. Il s'agit du noyau du morphisme d'évaluation $\varphi : K[X] \to \mathcal{L}(E)$, $P \mapsto P(f)$
De plus, $\frac{K[X]}{I} \xrightarrow{\sim} K[f] := \operatorname{Im}\varphi \subset \mathcal{L}(E)$

App ⑬: Soit $L : K$ une extension et $\varphi : K[X] \to L$ telle que $\begin{cases} \varphi_K \equiv id_K \text{ et } \varphi(X) = \alpha. \\ \varphi \text{ non injectif} \end{cases}$
Alors il existe $P \in K[X]$ tq $\ker\varphi = \langle P \rangle$ et $P(\alpha) = 0$ (α est dit algébrique)

prop ⑭: A est un corps ssi $A[X]$ est principal.

prop ⑮: si A est principal, on a pour tout idéal I :
I premier ssi I maximal

(c) Cas des anneaux euclidiens

def ⑯: A est dit euclidien s'il est muni d'une division euclidienne : $\exists \nu : A \setminus \{0\} \to \mathbb{N}$ tq $\forall a,b \in A$, $\exists q, r \in A$
$\begin{cases} a = bq + r \\ r = 0 \text{ ou } \nu(r) < \nu(b) \end{cases}$
ν est appelé stathme euclidien.

Exple ⑰: $(\mathbb{Z}, |\cdot|)$ est un anneau euclidien

prop ⑱: $K[X]$ est euclidien pour le stathme degré.

Thm ⑲ un anneau euclidien est principal.

Exple ⑳: $\mathbb{Z}[i]$ (entiers de Gauss) est euclidien

DEV (1)

prop(21) : si A euclidien, il existe $x \in A \setminus A^\times$ tel que $\pi : A \longrightarrow A/(x)$ restreinte à $A^\times \cup \{0\}$ soit surjective

C-exple(22) : $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal mais non euclidien.

II - Arithmétique dans les anneaux principaux

(a) Notion de divisibilité dans les D.I.

def(22) : soient $a, b \in A$. On dit que a divise b s'il existe $c \in A$ tq $ac = b$

prop(23) : $b | a$ ssi $(a) \subset (b)$

prop(24) : $(a) = (b)$ ssi $a | b$ et $b | a$ ssi $\exists c \in A^\times$ tq $a = cb$

on dit alors que a et b ~~sont associés~~.

def(25) • un élément $p \in A$ est dit irréductible si $p \notin A^\times$ et si $\left(\begin{matrix} p = ab \\ a, b \in A \end{matrix}\right. \Rightarrow a \in A^\times$ ou $b \in A^\times$

• un élément $p \in A$ est dit premier si :
$\forall a, b \in A$ tq $p | ab \Rightarrow p | a$ ou $p | b$

Exple(26) : le polynome minimal d'un polynome alg. est irréductible dans $K[X]$

prop(27) : un élément premier est irréductible.

Exple(28) : Dans $\mathbb{Z}[i\sqrt{5}]$, 2 est irréductible mais n'est pas principal.

(b) PGCD, PPCM et relation de Bezout

def(29) : Soient $a_1, \dots, a_n \in A^n$. On appelle pg.c.d. des $\{a_i\}_i$ tout élément $d \in A^*$ tq :

- $\forall i \leq n$, $d | a_i$
- $\forall c \in A^*$ $(\forall i \leq n, c | a_i \Rightarrow c | d)$

rmq : • le pgcd est definit à un inversible près.
• le pgcd d'un ensemble fini d'éléments n'existe pas necessairements.

C-exple(30) : 9 et $6 + 3i\sqrt{5}$ n'admettent pas de pgcd dans $\mathbb{Z}[i\sqrt{5}]$.

def(31) : soient $a_1, \dots, a_n \in A$. On appelle ppcm des $\{a_i\}_i$ tout élément $c \in A$ tq : • $\forall i \leq n$, $a_i | c$
• $\forall \tilde{c} \in A$ $(\forall i \leq n$ $a_i | \tilde{c} \Rightarrow c | \tilde{c})$

Thm (Bezout) : si A est principal et si $a, b \in A \setminus \{0\}$ et $d = \text{pgcd}(a, b)$. Alors : $(d) = (a) + (b)$

Thm (32) : l'existence du pgcd et du ppcm d'un ensemble fini d'éléments de A est avéré lorsque A est principal.

C-exple(33) : $K[X, Y]$ n'est pas principal. On a :

- $\text{pgcd}(X, Y) = 1$
- $(X) + (Y) = (X, Y) \neq (1) = K[X, Y]$

App(34) : (lemme des noyaux). Soient E un ev sur K ; $f \in \mathcal{L}(E)$ et $P = P_1 \times \dots \times P_r \in K[X]$ où les P_i sont 2 à 2 premiers entre eux. Alors :

$$\ker(P(f)) = \bigoplus_{i=1}^{r} \ker(P_i(f))$$

(c) Anneaux Factoriels

def(35) : un anneau intègre A est dit factoriel si
• $\forall a \in A \setminus \{0\}$, $a = \alpha \cdot \prod_{p \in \mathcal{P}} p^{\nu(p)}$ avec $\begin{cases} \alpha \in A^\times \\ \nu(p) \in \mathbb{N} \end{cases}$
et $\nu(p) = 0$ sauf un nbre fini de fois.
• cette décomposition est unique

C-exple(36) $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

Thm (37) : (lemme d'Euclide) si A est factoriel, alors :
$\begin{cases} p \text{ irréductible} \\ p \mid ab \end{cases} \Rightarrow p \mid a$ ou $p \mid b$

rmq (38) dans un anneau factoriel, premier $\Leftrightarrow$ irréduct.

App (39) : les polynomes cyclotomiques Φ_n sont irréductibles sur $\mathbb{Z}[X]$.

Thm (40) : (Gauss) Pour A factoriel, si $a \mid bc$ et si a est premier avec b, alors $a \mid c$

def (41) : soient $a, b \in A$. a et b sont dit premiers entre eux si $\forall d \in A$, $d \mid a$ et $d \mid b \Rightarrow d \in A^\times$

Thm (42) : un anneau principal est factoriel.

C-exple (43) : $\mathbb{Z}[X]$ (considérer l'idéal $\langle 2, X\rangle$)

intéressant si A $\rightarrow$ euclidien

(d) Lemme chinois

Thm (44) : soient A principal et $a_1, \dots, a_n \in A$ premiers entre eux 2 à 2. Alors $A/(a_1 \cdots a_n) \cong A/(a_1) \times \cdots \times A/(a_n)$

App (45) : Resolution d'un système de congruences :
$\begin{cases} x \equiv 2 \bmod 4 \\ x \equiv 3 \bmod 5 \\ x \equiv 1 \bmod 9 \end{cases}$ admet une unique solution modulo $180 = 4 \times 5 \times 9$

App (46) : soit $u \in \mathcal{L}(E)$.
u diagonalisable ssi $\exists \ell \in \mathbb{N}$ tq $K[u] \simeq K^\ell$

III - Entiers d'un corps quadratiques

(a) Généralités

def (47) : un corps quadratique K est une extension de $\mathbb{Q}$ de degré 2.

prop (48) : un corps quadratique est de la forme $\mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteurs carrés.

def (49) : on pose $\delta = \sqrt{d}$ et $z = x + y\delta \in \mathbb{Q}(\sqrt{d})$
- $\bar{z} = x - y\delta$ est le conjugué de z
- $N(z) = z\bar{z}$ norme de z.
- on dit que z est entier de $\mathbb{Q}(\delta)$ si son pol. minimal $P(X) = X^2 - 2x + x^2 - \delta^2 y^2 \in \mathbb{Z}[X]$ ie $\begin{cases} 2x \in \mathbb{Z} \\ N(z) \in \mathbb{Z} \end{cases}$

on note A_d l'ensemble des entiers de $\mathbb{Q}(\sqrt{d})$

prop (50) :
- A_d sous-anneau de $\mathbb{Q}(\delta)$
- si $d \equiv 2$ ou $3 \bmod 4$, $A_d = \mathbb{Z} + \delta \cdot \mathbb{Z}$
- si $d \equiv 1 \bmod 4$ $A_d = \mathbb{Z} + \mathbb{Z}\cdot\theta$ où $\theta = \frac{1+\delta}{2}$
- si $d < 0$, N est un stathme euclidien ssi $d \in \{-1, -2, -3, -7, -11\}$

App (51) : (equation de Mordell) : $y^2 = x^3 - 1$ admet $(1, 0)$ comme unique solution.

(b) Entiers de Gauss $\mathbb{Z}[i]$

def (52) : on note $\Sigma := \{n \in \mathbb{N},\ n = a^2 + b^2,\ a, b \in \mathbb{N}\}$

prop (53) : $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Thm (2 carrés) : $p \in \Sigma$ et premier
ssi p n'est pas irréductible dans $\mathbb{Z}[i]$
ssi $p = 2$ ou $p \equiv 3 \bmod 4$
DEV 2

Thm (55) : les irréductibles de $\mathbb{Z}[i]$ sont, à inversible près,
- les entiers premiers $p \in \mathbb{N}$ tq $p \equiv 3 \bmod 4$
- les entiers de Gauss $a + ib$ dont la norme est un nbre premier.

- J. Calais "Eléments de Théorie des anneaux"
- D. Perrin "Cours d'algèbre" (pour les deux dev.)
- R. Goblot "Alg. Commut." (résultat sur les idéaux premiers de $K[X,Y]$)
-

THÉORÈME DES 2 CARRÉS

Ref. Perrin, "Cours d'Algèbre"

Notations • $\mathbb{Z}[i] = \{a+ib,\ a,b \in \mathbb{Z}\} \subset \mathbb{C}$

• $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$
$\quad z = a+ib \longmapsto a^2+b^2$ est multiplicative

• $\Sigma = \{n \in \mathbb{N},\ n = a^2+b^2,\ a,b \in \mathbb{N}\}$

Prop $\mathbb{Z}[i]^\times = \{\pm 1 ; \pm i\}$

Dem : Soit $z \in \mathbb{Z}[i]^\times$, $\exists z' \in \mathbb{Z}[i]^\times$, $zz' = 1 \Rightarrow N(z)N(z') = 1$
$\Rightarrow N(z) = 1$

Si $z = a+ib$, $a,b \in \mathbb{Z}$, $N(z) = 1$

$$\Leftrightarrow a^2+b^2 = 1$$

$$\Leftrightarrow \begin{cases} a=0 \text{ et } b = \pm 1 \\ \text{ou} \\ a = \pm 1 \text{ et } b = 0 \end{cases}$$

D'où $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Prop $\mathbb{Z}[i]$ est euclidien de stathme N

Dem : Soit $z, t \in \mathbb{Z}[i]$ tels que $\frac{z}{t} = x+iy \in \mathbb{C}$, $x,y \in \mathbb{R}$

Soient $a,b \in \mathbb{Z}$ tels que $|x-a| \leq \frac{1}{2}$ et $|y-b| \leq \frac{1}{2}$

On pose $q = a+ib$ et alors $\left|\frac{z}{t} - q\right| = |x-a+i(y-b)|$

$$\leq \frac{\sqrt{2}}{2} < 1$$

Soit $r = z - qt \in \mathbb{Z}[i]$ car anneau

$r = t\left(\frac{z}{t} - q\right)$ d'où $|r| < |t| \Rightarrow |r|^2 < |t|^2$

$$\Rightarrow N(r) < N(t)$$

On a donc $z = qt + r$ avec $N(r) < N(t)$ d'où l'euclidiennité.

Thm Soit p un nombre premier. On a équivalence entre
1) $p \in \Sigma$
2) p non irréductible dans $\mathbb{Z}[i]$
3) $p = 2$ ou $p \equiv 1 \bmod 4$.

Dem : $\boxed{1 \Leftrightarrow 2}$ $\Rightarrow$ $p \in \Sigma$ donc $p = a^2 + b^2$, $a, b \in \mathbb{N}^*$

$= (a+ib)(a-ib)$

$a+ib$ et $a-ib$ non inversibles car a, b non nuls, donc p non irréductible dans $\mathbb{Z}[i]$

$\Leftarrow$ Soit $p = zz'$ où $z, z' \in \mathbb{Z}[i] \setminus \{\pm 1, \pm i\}$

$N(p) = N(z)N(z') = p^2$. Or $N(z) \neq 1$ car z non inversible donc $N(z) = p$

Comme $z = a+ib \in \mathbb{Z}[i]$, $N(z) = a^2 + b^2 \in \Sigma$

$\boxed{2 \Leftrightarrow 3}$ • Si $p = 2$, $p = 1^2 + 1^2$.

• Supposons $p > 2$

p non irréductible dans $\mathbb{Z}[i]$ $\Leftrightarrow$ p non premier dans $\mathbb{Z}[i]$ par factorialité

$\Leftrightarrow$ (p) non premier

$\Leftrightarrow$ $\dfrac{\mathbb{Z}[i]}{(p)}$ non intègre

Or $\dfrac{\mathbb{Z}[i]}{(p)} \simeq \dfrac{\mathbb{Z}[X]/(X^2+1)}{(p)} \simeq \dfrac{\mathbb{Z}/p\mathbb{Z}[X]}{(X^2+1)}$

Ainsi, (p) non premier $\Leftrightarrow$ X^2+1 non irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$

$\Leftrightarrow$ X^2+1 admet une racine dans $\mathbb{Z}/p\mathbb{Z}[X]$

$\Leftrightarrow$ -1 carré de $\mathbb{Z}/p\mathbb{Z}$

$\Leftrightarrow$ $(-1)^{\frac{p-1}{2}} = 1$

$\Leftrightarrow$ $\dfrac{p-1}{2}$ pair

$\Leftrightarrow$ $p \equiv 1 \mod 4$.

Lme : $x \in (\mathbb{F}_p^*)^2$ si et seulement si $x^{\frac{p-1}{2}} = 1$

$\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ EST PRINCIPAL, PAS EUCLIDIEN

Ref : Perrin

Prop① (pseudo-division euclidienne) Soit $A = \mathbb{Z}[\alpha]$

Soient $a, b \in A \setminus \{0\}$. Alors $\exists\, q, r \in A$, $a = bq + r$ ou $2a = bq + r$
avec $r = 0$ ou $\nu(r) < \nu(b)$ pour ν stathme de A

On pose $A = \mathbb{Z}[\alpha]$ où $\alpha = \frac{1+i\sqrt{19}}{2}$

Etude de A : * $\left(\alpha - \frac{1}{2}\right)^2 = -\frac{19}{4}$ donc α est racine de $P = X^2 - X + 5$

* $\bar{\alpha} = 1 - \alpha \in A$

* Pour $z = a + b\alpha \in A$, $N(z) = z\bar{z}$

$$= (a + b\alpha)(a - b\bar{\alpha})$$
$$= a^2 + ab(\alpha + \bar{\alpha}) + b^2 \alpha\bar{\alpha}$$

avec $\alpha\bar{\alpha} = \frac{1}{4} + \frac{19}{4} = 5$ et $\alpha + \bar{\alpha} = 1$.

Ainsi $\boxed{N(z) = a^2 + ab + 5b^2}$

* Si $z \in A^\times$, $N(z) = 1 \Rightarrow \left(a + \frac{b}{2}\right)^2 + \frac{19}{4} b^2 = 1$

$$\Rightarrow \begin{cases} b = 0 \\ a = \pm 1 \end{cases} \quad \text{donc } A^\times = \{\pm 1\}$$

Prop② : A n'est pas euclidien

Dem : Raisonnons par l'absurde. Si A est euclidien, par la proposition 21, il existe $x \in A \setminus A^\times$ tel que $\pi : A \to A/(x)$, restreinte à $A^\times \cup \{0\}$ est surjective, ie $|A/(x)| \leq |A^\times \cup \{0\}| = 3$

Or $A \neq \phi$ donc $|A/(x)| = 2$ ou 3 et $A/(x) \simeq \mathbb{F}_2$ ou $\mathbb{F}_3$ car c'est un corps fini.

On pose alors $\varphi : A \to \mathbb{K}$ de noyau (x).

Si $\beta = \varphi(\alpha)$, on a par propriété de morphisme : $\beta^2 - \beta + 5 = 0$

Or cette équation n'a aucune solution dans $\mathbb{F}_2$ ou $\mathbb{F}_3$.

Donc A ne peut pas être euclidien ■

Prop | A est un anneau principal

Dem $A \simeq \frac{\mathbb{Z}[X]}{(P)}$ donc $\frac{A}{(2)} \simeq \frac{\mathbb{Z}[X]/(P)}{(2)} \simeq \frac{\mathbb{Z}/2\mathbb{Z}[X]}{(P)}$

P est de degré 2 et sans racine dans $\mathbb{Z}/2\mathbb{Z}$ donc irréductible

Donc $A/(2)$ est un corps et (2) est maximal dans A

- Soit $I \neq (0)$ un idéal de A et $a \in I \setminus \{0\}$ de norme minimale

~~Supposons~~ $x \in I \setminus (a)$

Par la proposition ①, $x = aq + r$ ou $2x = aq + r$ avec $r = 0$ ou $N(r) < N(a)$

Or $N(a)$ minimale et $r = 2x - aq \in I$ donc $r = 0$.

Si $x = aq \in (a)$ on aboutit à une contradiction !

Si $2x = aq$, $aq \in (2)$ maximal et ainsi premier

Alors $a \in (2)$ ou $q \in (2)$. Si $q \in (2)$, $\exists q'$, $q = 2q'$ et $x = aq' \in (a)$ ↯

Donc $a = 2a'$ et $q \notin (2)$. Ainsi $x = a'q$.

- Par maximalité de (2), $(2, q) = A$ et il existe $(\lambda, \mu) \in A^2$ tel que

$2\lambda + q\mu = 1 \Rightarrow 2\lambda a' + q\mu a' = a'$

$\Rightarrow \lambda a + \mu x = a' \in I$

Or $N(a') < N(a)$ donc on a aussi une contradiction.

- On en déduit que $I = (a)$ et A est principal ■