Anneaux principaux et applications.

122

[Ram] IX.1 VIII.2 VIII.1 VIII.5 [Ram]

Soit A anneau, $n \in \mathbb{N}^*$, $\mathbb{K}$ corps commutatif.

I] Notion de principalité

1] Idéaux et anneaux principaux

Définition 1: Soit $a \in A$. L'ensemble $\langle a \rangle = \{qa \mid q \in A\}$ est un idéal appelé idéal principal engendré par a.

Exemple 2: $n\mathbb{Z}$ est un idéal principal de $\mathbb{Z}$.

Contrexemple 3: $\langle 2; X \rangle$ n'est pas principal dans $\mathbb{Z}[X]$.

Définition 4: On dit que A est principal s'il est intègre et si tout idéal de A est principal.

Exemple 5: Un corps est un anneau principal (les idéaux sont $\langle 0 \rangle$ et $\langle 1 \rangle$).

Théorème 6: Tout sous-anneau de $\mathbb{Q}$ est principal

Exemple 7: L'anneau $\mathbb{D}$ des nombres décimaux est principal.

Théorème 8: Soit $S \subset A^*$ contenant 1 stable par multiplication et $S^{-1}A = \left\{ \frac{a}{s} \mid a \in A, s \in S \right\}$.

Alors: $S^{-1}A$ est un sous-anneau de $\mathrm{Frac}(A)$

De plus, si A est principal, alors $S^{-1}A$ est principal.

Exemple 9: (1) Pour $A = \mathbb{Z}$ et $S = \{10^n \mid n \in \mathbb{N}\}$, on retrouve que $\mathbb{D}$ est principal.

(2) Pour $A = \mathbb{K}[X]$, $S = \{X^n \mid n \in \mathbb{N}\}$, on a que l'anneau $S^{-1}A = \left\{ \frac{P(X)}{X^n} \mid P \in \mathbb{K}[X], n \in \mathbb{N} \right\}$ est principal.

2] Anneaux euclidiens

Définition 10: Un anneau commutatif et intègre A est dit euclidien s'il existe une application stathme: $\varphi : A^* \to \mathbb{N}$ telle que

(i) $\forall a, b \in A \times A^*$, $\exists q, r \in A^2 \mid a = bq + r$

(ii) $r = 0$ ou $(r \neq 0$ et $\varphi(r) < \varphi(b))$

On dit que le stathme est croissant si $\forall a, b \in A^{*2}$, $\varphi(ab) \geq \varphi(a)$.

Théorème 11: Un anneau euclidien est principal. Plus précisément, pour tout $\{0\} \neq I \subset A$ idéal, il existe $a_0 \in I \setminus \{0\}$ tel que $\varphi(a_0) = \min_{a \in I \setminus \{0\}} \{\varphi(a)\}$ et $I = a_0 A$.

Proposition 12: L'anneau $\mathbb{Z}$ est euclidien par $\varphi : \mathbb{Z}^* \to \mathbb{N}$, $n \mapsto |n|$

Proposition 13: Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est euclidien.

Proposition 14: Soit A anneau commutatif, unitaire, intègre.

Alors: $A[X]$ est principal ssi A est un corps

Exemple 15: $\mathbb{K}[X;Y]$ n'est pas principal car $\mathbb{K}[X]$ n'est pas un corps.

3] Anneaux d'entiers

Théorème 16: L'anneau $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ est euclidien par $\varphi : \mathbb{Z}[i] \to \mathbb{N}$, $a + ib \mapsto a^2 + b^2$.

Application 17: (Théorème de Fermat) Un nombre premier p est somme de deux carrés ssi $p = 2$ ou $p \equiv 1 \ [4]$.

Proposition 18: $\mathbb{Z}[i\sqrt{n}] = \{a + ib\sqrt{n} \mid a, b \in \mathbb{Z}\}$ est euclidien ssi $n \in \{1; 2\}$.

Proposition 19: $\mathbb{Z}[\omega] = \{a + ib \mid a, b \in \mathbb{Z}\}$ est un anneau ssi ω est une racine de polynôme sur $\mathbb{Z}$ de degré 2.

Contrexemple 20: $\mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right]$ est un anneau principal, non-euclidien.

II] Arithmétique dans les anneaux principaux

1] Divisibilité, éléments premiers et irréductibles

Définition 21: Soit $a, b \in A$. On dit que a divise b s'il existe $c \in A$ tel que $b = ac$. On note $a \mid b$

Proposition 22: $b \mid a$ ssi $(a) \subset (b)$

Remarque 23: (1) Tout élément $a \in A$ divise 0

(2) Tout élément $a \in A^\times$ divise tous les éléments de A.

On suppose par la suite A un anneau intègre.

IX.4.1 [Ram] VIII.1 IX.4.3 IX.4.4 [Ram]

VII.1 [Rou] VII.6 [Rou] VIII.1

Définition 24 : Un élément $p \in A^* \setminus A^\times$ est dit irréductible si : $(p = ab) \Rightarrow (a \in A^\times$ ou $b \in A^\times)$

Remarque 25 : Dans un corps il n'y a pas d'élément irréductible.

Définition 26 : Un élément $p \in A^* \setminus A^\times$ est dit premier si :
$(p \mid ab) \Rightarrow (p \mid a$ ou $p \mid b)$

Lemme 27 : (d'Euclide) Dans un anneau factoriel, un élément est irréductible ssi il est premier. Ceci est en particulier vrai dans les anneaux principaux.

Exemple 28 : Pour $n \geq 3$, les anneaux $\mathbb{Z}[i\sqrt{n}]$ ne sont pas factoriels puisque 2 est irréductible, non-premier.

Proposition 29 : Soit A anneau principal, $\{0\} \neq I \neq A$ idéal
Alors : $\frac{A}{I}$ est principal ssi a est premier ou irréductible

2) PGCD, relation de Bezout et réduction dans les anneaux euclidiens

Définition 30 : Soit $(a_i)_{i=1}^r \in A^{*r}$. On dit que les (a_i) admettent un plus grand commun diviseur (PGCD) si :
$\exists \delta \in A^* \mid \forall k \in [\![1;r]\!]$, $\delta | a_k$ et tout diviseur commun à $a_1, \dots, a_r$ divise δ.
On dit que A est un anneau à PGCD si deux éléments quelconques de A admettent un PGCD.

Théorème 31 : Tout anneau principal est un anneau à PGCD.
Précisément, pour tout $(a_i)_{i=1}^r \in A^{*r}$, $\exists \delta \in A^* \mid \langle a_1, \dots, a_r \rangle = \langle \delta \rangle$ avec $\delta = \sum_{k=1}^r u_k a_k$ avec $(u_i)_{i=1}^r \in A^r$ et $\delta = a_1 \wedge \dots \wedge a_r$.

Théorème 32 : (de Gauss) Soit A anneau à PGCD, $a, b \in A^*$.
Alors : a et b sont premiers entre eux ssi $\forall c \in A^*$, $a | bc \Rightarrow a | c$.

Théorème 33 : (de Bézout) Soit $(a_i)_{i=1}^r \in A^*$ avec A principal
Alors : $a_1 \wedge \dots \wedge a_r = 1$ ssi $\exists (u_i)_{i=1}^r \in A^r \setminus \sum_{i=1}^r u_i a_i = 1$.

Remarque 34 : On utilise l'algorithme d'Euclide étendu pour trouver les u_i dans un anneau euclidien.

Application 35 : (forme normale de Smith) Soit A anneau euclidien, $m, n \in \mathbb{N}^*$, $M \in \mathcal{M}_{m,n}(A)$
Alors : $\exists P, Q \in GL_m(A) \times GL_n(A) \setminus PMQ = \begin{pmatrix} f_1 & & \\ & \ddots & \\ & & f_r \end{pmatrix}$ avec $f_1 | \dots | f_r \in A^r$ tels que $f_1 \wedge \dots \wedge f_r$ uniques modulo les inversibles de A.

VIII.2 [Rou] VIII.3 [Rou] [Les] [Tsar]

3) Lemme des restes chinois

Lemme 36 : Soit A anneau principal, $(a_i)_{i=1}^r \in A^* \setminus A^\times$, $a = \prod_{i=1}^r a_i$ avec (a_i) deux à deux premiers entre eux, $\left(b_j = \frac{a}{a_j} = \prod_{i \neq j} a_i\right)_{j=1}^r$
Alors : les (b_j) sont premiers entre eux.

Théorème 37 : (des restes chinois) Soit A anneau principal, $(a_i)_{i=1}^r \in A^* \setminus A^\times$ deux à deux premiers entre eux, $a = \prod_{i=1}^r a_i$.
Alors : l'application $\varphi : \begin{array}{ccc} A & \to & \prod_{i=1}^r A/\langle a_i \rangle \\ x & \mapsto & (\pi_1(x), \dots, \pi_r(x)) \end{array}$ est un morphisme d'anneaux surjectif de noyau $\ker(\varphi) = \langle a \rangle$ qui induit un isomorphisme d'anneaux $\Psi : \begin{array}{ccc} A/\langle a \rangle & \to & \prod_{i=1}^r A/\langle a_i \rangle \\ x & \mapsto & (\pi_1(x), \dots, \pi_r(x)) \end{array}$ d'inverse $\Psi^{-1} : \begin{array}{ccc} \prod_{i=1}^r A/\langle a_i \rangle & \to & A/\langle a \rangle \\ (\pi_1(x_1), \dots, \pi_r(x_r)) & \mapsto & \sum_{i=1}^r x_i u_i b_i \end{array}$ avec $(u_i) \in A$ telle que : $\sum_{i=1}^r u_i b_i = 1$.

Proposition 38 : Soit $S : \begin{array}{ccc} \mathbb{F}_q[X] & \to & \mathbb{F}_q[X] \\ Q & \mapsto & Q^q \end{array}$ avec $q = p^n$ avec p premier et $n \in \mathbb{N}$ est un $\mathbb{F}_q$-endomorphisme.

Lemme 39 : Soit $\mathbb{L}$ extension de $\mathbb{F}_q$ et $x \in \mathbb{L}$.
Alors : $x^q = x$ ssi $x \in \mathbb{F}_q$

[Tsen]

Théorème 40 : (de Berlekamp) Soit $q = p^n$ avec p premier $n \in \mathbb{N}$, $P \in \mathbb{F}_q[X]$ sans facteur carré et $P = \prod_{i=1}^{r} P_i$ sa décomposition en irréductibles de $\mathbb{F}_q[X]$.

Alors : (1) Si $r = 1$, alors P est irréductible.

(2) Sinon, il existe $a \in \mathbb{F}_q$, $V \in \mathbb{F}_q[X]$ tel que :
PGCD$(P, V-a)$ est facteur non-trivial de P.

Références :

[Rom] Mathématiques pour l'agrégation Algèbre et Géométrie — Rombaldi

[Les] 131 développements pour l'oral — Lesesvre

[Isen] L'oral à l'agrégation de mathématiques — Isenmann