Anneaux principaux. Exemples et applications.

122

Un anneau A est dit principal s'il est intègre (donc commutatif) et si tout idéal est principal.
exples : $\mathbb{Z}$, $K[X]$, $K[[X]]$ (où K est un corps), $\mathbb{Z}[i]$.
contre-exples : $(2,X)$ n'est pas principal dans $\mathbb{Z}[X]$; (X,Y) n'est pas principal dans $\mathbb{R}[X,Y]$; $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre (bien que tout idéal soit principal).
Dans la suite, A désigne un tel anneau.

I) Propriétés arithmétiques

1) Divisibilité

déf : soient $a, b \in A$. On dit que a divise b, et on écrit $a|b$, s'il existe $c \in A$ tel que $b = ac$, ie $(b) \subset (a)$.
déf : on dit que a et b sont associés si $(a) = (b)$ ie (A étant intègre) s'il existe $u \in A^\times$ tq $a = ub$. On définit ainsi une relation d'équivalence $\mathcal{R}$ sur A : $a \mathcal{R} b$ ssi $(a) = (b)$.

Notons $I(A)$ l'ensemble des idéaux de A. On a :

Prop : $(A/\mathcal{R}, |) \simeq (I(A), \supset)$ (isomorphisme d'ens. ordonnés)

déf : les éléments de $I(A)\backslash\{A\}$ maximaux pour l'inclusion sont appelés idéaux maximaux.
exple : les idéaux maximaux de $\mathbb{Z}$ sont les (p) avec $p \in \mathbb{P}$.
Prop : un idéal I est maximal si A/I est un corps.

On définit aussi les idéaux premiers :

déf : I est dit premier si A/I est intègre.
déf équivalente : I est dit premier si :
i) $A \neq I$
ii) $\forall a, b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$

On peut maintenant définir les notions d'éléments irréductible et premier :

déf : i) on dit que p est premier si $p \neq 0$ et si (p) est un idéal premier.
ii) on dit que p est irréductible si $p \neq 0$ et si (p) est un idéal maximal.

déf équivalente à ii) : p est irréductible si $p \notin A^\times$ et si $p = ab \Rightarrow a \in A^\times$ ou $b \in A^\times$.

Rqe : dans le cadre de cette leçon (A principal), les notions coïncident, ie p est premier ssi p est irréductible.

Prop : un idéal $I \neq \{0\}$ est premier ssi il est maximal.

déf : $\forall a, b \in A\backslash\{0\}$, on appelle pgcd de a et b tout générateur de l'idéal $(a) + (b)$ et ppcm de a et b tout générateur de l'idéal $(a) \cap (b)$.
Si $(d) = (a) + (b)$, les éléments $\lambda, \mu \in A$ tels que $d = \lambda a + \mu b$ sont appelés coefficients de Bézout.

déf : on dit que a et b sont premiers entre eux si $\text{pgcd}(a,b) = 1$, ie si l'on a :
$\forall d \in A$ $d|a$ et $d|b \Rightarrow d \in A^\times$.

2) Factorialité

Théorème de Gauss : si $a | bc$ et si $a \wedge b = 1$ alors $a | c$.

Lemme d'Euclide : si p est irréductible et si $p | ab$, alors $p | a$ ou $p | c$.

Tout anneau principal possède la propriété suivante :

Prop : il existe un ensemble $P \subset A$ d'éléments irréductibles qui est tel que :

i) $\forall a \in A\setminus\{0\}$, a s'écrit sous la forme

$$a = u \prod_{p \in P} p^{\nu_p(a)} \text{ avec } u \in A^\times, \nu_p(a) \in \mathbb{N}$$

et $\exists I$ fini $\subset P$ tq $\forall p \in P\setminus I$ $\nu_p(a) = 0$.

ii) l'écriture est unique.

Remarque : un anneau intègre qui vérifie i) et ii) se dit factoriel. De plus, si i) est vérifiée, ii) équivaut au lemme de Gauss ou d'Euclide.

On peut reformuler les déf du pgcd et du ppcm :

Prop: si $a = u \prod p^{\nu_p(a)}$ et $b = v \prod p^{\nu_p(b)}$ alors un pgcd de a et b est donné par $\prod p^{\min(\nu_p(a), \nu_p(b))}$ et un ppcm est donné par $\prod p^{\max(\nu_p(a), \nu_p(b))}$.

Théorème chinois: soit $a \in A$ que l'on écrit en produit d'irréductibles $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$, alors

$$A/(a) \simeq \prod_{i=1}^{n} A/(p_i^{\alpha_i})$$

3) Anneaux euclidiens

déf : un anneau A intègre est dit euclidien s'il existe une fonction $\nu : A\setminus\{0\} \to \mathbb{N}$ telle que si $a, b \in A\setminus\{0\}$, il existe $q, r \in A$ avec $a = bq + r$ et $r = 0$ ou $\nu(r) < \nu(b)$.

exple : $\mathbb{Z}$ avec $\nu = |\cdot|$, $K[X]$ et $\nu = \deg$.

Prop : tout anneau euclidien est principal.

contre-exemple : l'anneau $\mathbb{Z}\left[\frac{1}{2}(1+i\sqrt{19})\right]$ est principal mais non euclidien.] DEV 1

II) Exemples et applications

1) $\mathbb{Z}$: $\mathbb{Z}^\times = \{\pm 1\}$ et $\{\text{irréductibles}\} = \mathcal{P}$

2) $K[X]$ où K est un corps :

Prop : soit A un anneau. $A[X]$ est principal ssi A est un corps.

Prop : si K est un corps, $K[X]$ est euclidien. En revanche, $K[X_1, \dots, X_n]$ n'est pas euclidien ni même principal. **Exemple** : (X, Y) n'est pas un idéal principal de $K[X, Y]$.

Prop : $K[X]^\times = K^*$

* **Éléments irréductibles et adjonction de racines** :

Prop : $P \in \mathbb{R}[X]$ est irréductible si $\deg P = 1$ ou $\deg P = 2$ et $\Delta < 0$.

Application : X^2+1 est irréductible dans $\mathbb{R}[X]$ qui est un anneau euclidien, donc principal, donc (X^2+1) est un idéal maximal et $\mathbb{R}[X]/(X^2+1)$ est un corps. On pose $\mathbb{C} := \mathbb{R}[X]/(X^2+1)$.

Prop : soit $\mathbb{F}_p$ un corps fini. $\forall n \geq 1$, il existe un polynôme P irréductible dans

$\mathbb{F}_p[X]$ de degré n. On pose $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(P)$.

exple : $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$.

* Applications en algèbre linéaire :

Prop : soit E un ev de dimension finie sur un corps K. Soit $u \in \mathcal{L}(E)$, on définit l'application $\varphi_u : K[X] \longrightarrow \mathcal{L}(E)$, $P \longmapsto P(u)$.
$\ker(\varphi_u) \neq \{0\}$ est un idéal de l'anneau principal $K[X]$ donc $\exists\, \pi_u \in K[X]$ unitaire tel que $\ker(\varphi_u) = \pi_u$. π_u est appelé polynôme minimal de u.

Prop : u est diagonalisable ssi π_u est scindé à racines simples sur K.

Lemme des noyaux : soit $P = P_1 \cdots P_r$ avec $\forall\, i \neq j$ $P_i \wedge P_j = 1$, alors on a :
$$\ker P(u) = \bigoplus_{i=1}^{n} \ker P_i(u).$$

3) $\mathbb{Z}[i]$

$\mathbb{Z}[i] = \{a+ib / a,b \in \mathbb{Z}\}$. On définit la norme $N : \mathbb{Z}[i] \longrightarrow \mathbb{N} : z \mapsto z\bar{z}$.

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

Prop : $\mathbb{Z}[i]$ est un anneau euclidien relativement à la fonction N.

V2 Th : soit $p \in \mathcal{P} \cap \mathbb{N}$, alors p est somme de 2 carrés ssi $p = 2$ ou $p \equiv 1\ [4]$, et $\forall\, n \in \mathbb{N}^*$, n est somme de deux carrés ssi $\forall\, p \in \mathcal{P}$ $p \equiv 3\ [4] \Rightarrow v_p(n)$ est pair.

Prop : les irréductibles de $\mathbb{Z}[i]$ sont, aux inversibles près, les $p \in \mathcal{P} \cap \mathbb{N}$ tq $p \equiv 3\ [4]$ et les $z \in \mathbb{Z}[i]$ tq $N(z) \in \mathcal{P} \cap \mathbb{N}$.

4) $\mathbb{Z}[j] = \{a+jb / (a,b) \in \mathbb{Z}^2\}$

Prop : $\mathbb{Z}[j]$ est un anneau euclidien relativement à N. Les inversibles sont $\{\pm 1, \pm j, \pm j^2\}$ ie les racines 6è de l'unité

Application : Équation de Fermat pour $n=3$

L'équation $x^3 + y^3 = z^3$ n'a pas de solution $(x,y,z) \in (\mathbb{Z}^*)^3$.

5) $K[[X]]$

Prop : $K[[X]]$ est un anneau euclidien, muni de la valuation v définie ci-après si $A = \sum_{i \in \mathbb{N}} a_i X^i$, $v(A) = \min\{i \in \mathbb{N}, a_i \neq 0\}$.

- Les inversibles sont les éléments dont le terme de degré 0 est $\neq 0$.
- X est le seul élément irréductible, à inversible près.

Leçon 122: Anneaux principaux. Exemples et applications.

Quentin Garchery

19 mai 2015

1 Théorème des deux carrés

On note $\Sigma = \{a^2 + b^2, (a,b) \in \mathbb{N}^2\}$ et soit p un nombre premier.

Théorème 1. *$p \in \Sigma \iff p = 2$ ou $p \equiv 1[4]$*

Démonstration.
On va raisonner par équivalence : soit (P1) la propriété '$p \in \Sigma$'. On considère l'anneau $\mathbb{Z}[i]$ qu'on va munir de la 'norme' N : pour $z \in \mathbb{Z}[i], N(z) = |z|^2$. On voit facilement que les éléments inversibles de $\mathbb{Z}[i]$ sont les éléments de norme 1 et cela nous permet de caractériser les éléments irréductibles de $\mathbb{Z}[i]$.
(P1) est équivalente à p n'est pas irréductible dans $\mathbb{Z}[i]$. En effet soit alors $p \in \Sigma$, $\exists (a,b) \in \mathbb{N}^2, p = a^2 + b^2 = (a + bi)(a - bi)$ et $a + bi$ et $a - bi$ ne sont pas inversibles. Réciproquement si $p = \alpha\beta$ avec α et β de norme différente de 1 alors $N(\alpha)|N(p) = p^2$ donc $N(\alpha) = p$, p est somme de deux carrés.
Puisque $\mathbb{Z}[i]$ est principal, (P1) est équivalente à (p) n'est pas premier. Par l'isomorphisme $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2 + 1)$, cela veut dire que (p) n'est pas premier dans $\mathbb{Z}[X]/(X^2+1)$. Or $(\mathbb{Z}[X]/(X^2+1))/(p) \cong \mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$ et $\mathbb{Z}/p\mathbb{Z}[X]$ est principal d'où l'équivalence avec le fait que X^2+1 n'est pas irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$. C'est-à-dire que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$. On a donc que (P1) est équivalente à $p = 2$ ou $(-1)^{(p-1)/2} = 1$.

□

On a utilisé les propositions :

Proposition 1.1. *Soit A un anneau et $\alpha, \beta \in A$. On note $\overline{\beta}$ la classe de β modulo α. On a l'isomorphisme :*

$$A/(\alpha, \beta) \cong (A/(\alpha))/(\overline{\beta})$$

Démonstration. Soient $\Pi_\alpha : A \to A/(\alpha)$ et $\Pi_{\overline{\beta}} : A/(\alpha) \to (A/(\alpha))/(\overline{\beta})$ les projections canoniques. $\Pi_{\overline{\beta}} \circ \Pi_\alpha$ est surjective et son noyau est :

$$\begin{aligned} Ker(\Pi_{\overline{\beta}} \circ \Pi_\alpha) &= \{a \in A, \overline{a} \in (\overline{\beta})\} \\ &= \{a \in A, \exists u \in A, \overline{a} = \overline{u\beta}\} \\ &= \{a \in A, \exists u, v \in A, a = u\beta + v\alpha\} \\ &= (\alpha, \beta) \end{aligned}$$

□

Proposition 1.2. *Si $p \neq 2$, s'équivalent :*
(i) x est un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$
(ii) $x^{\frac{p-1}{2}} = 1$

2 Un exemple d'anneau principal non-euclidien

Posons $\alpha = \frac{1+i\sqrt{19}}{2}$ et $\mathbf{A} = \mathbb{Z}[\alpha]$.

Théorème 2. **A** *est principal et n'est pas euclidien.*

Démonstration. On a $\alpha\overline{\alpha} = 5$ et $\alpha + \overline{\alpha} = 1$ donc $\alpha^2 - \alpha + 5 = 0$ ce qui nous permet de montrer que $\mathbf{A} = \{a + b\alpha, a, b \in \mathbb{Z}\}$.

A est intègre comme sous-anneau de $\mathbb{C}$. De plus la relation $\alpha + \overline{\alpha} = 1$ nous montre qu'il est stable par passage au conjugué. On définit alors la 'norme' N sur cet anneau, pour $z = a + b\alpha$:

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

N est multiplicative, ce qui donne, pour un élément $z = a + b\alpha \in \mathbf{A}^\times$:
$N(zz^{-1}) = N(z)N(z^{-1}) = 1$. Donc $N(z) = 1$ c'est-à-dire

$$(a + b/2)^2 + \frac{19}{4}b^2 = 1$$

D'où $\frac{19}{4}b^2 \leq 1$ puis $b = 0$. On en déduit $a = \pm 1$ et on vérifie que $\mathbf{A}^\times = \{\pm 1\}$.

Montrons que **A** n'est pas euclidien par l'absurde : soit ν un stathme.
Soit x un élément de **A** de stathme minimal parmi les éléments non inversibles. Alors le reste de la division euclidienne d'un élément a de **A** par x donne un élément inversible ou nul. Donc la restriction à $\mathbf{A}^\times \cup \{0\}$ de la projection canonique de **A** sur $\mathbf{A}/(x)$ est surjective. On a donc un morphisme surjectif de **A** dans un

anneau de cardinal 2 ou 3 (car x n'est pas inversible) où tout élément non nul est l'image d'un élément inversible donc est inversible. L'image β de α par ce morphisme vérifie : $\beta^2 - \beta + 5 = 0$. Mais cette équation n'a pas de solutions dans $\mathbb{Z}/3\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z}$, d'où une contradiction.

Montrons aussi que $\mathbf{A}$ est principal. Pour cela on va d'abord prouver qu'on peut munir $\mathbf{A}$ d'une sorte de division euclidienne : si $a, b \in \mathbf{A} - \{0\}$,

[1] soit $\exists q, r \in \mathbf{A}$ tels que $a = bq + r$ et $r = 0$ ou $N(r) < N(b)$

[2] soit $\exists q, r \in \mathbf{A}$ tels que $2a = bq + r$ et $r = 0$ ou $N(r) < N(b)$.

Faisons déjà la division dans $\mathbb{C}$:

$$x = \frac{a}{b} = \frac{a\overline{b}}{b\overline{b}} \in \mathbb{Q}[\alpha]$$

On écrit $x = u + v\alpha$ avec $u, v \in \mathbb{Q}$ avec $v \in [n, n+1[$.

• On suppose d'abord que $v \notin]n + \frac{1}{3}, n + \frac{2}{3}[$. Soient s l'entier le plus proche de u et t l'entier le plus proche de v. Alors

$$N(x - (s + t\alpha)) = (s-u)^2 + (s-u)(t-v) + 5(t-v)^2 \leq \frac{1}{2^2} + \frac{1}{2} \times \frac{1}{3} + \frac{5}{3^2} < 1.$$

Si on pose $q = s + t\alpha$ et $r = a - bq$ alors $r = 0$ ou $N(r) = N(b)N(x-q) < N(b)$.

• Si maintenant $v \in]n + \frac{1}{3}, n + \frac{2}{3}[$ alors $2v \in]2n + \frac{2}{3}, 2n + 1 + \frac{1}{3}[=]2n + \frac{2}{3}, 2n + 1[\cup [2n+1, 2n+1+\frac{1}{3}[$. En considérant $x' = 2x, a' = 2a, u' = 2u, v' = 2v$, on se ramène au cas précédent.

On a $\alpha^2 - \alpha + 5$. Par division euclidienne on en déduit que $\mathbf{A}$ est isomorphe à $\mathbb{Z}[X]/(X^2 - X + 5)$, et, en utilisant le premier théorème d'isomorphisme :

$$\mathbf{A}/(2) \simeq \mathbb{Z}[X]/(2, X^2 - X + 5) \simeq (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 + X + 1).$$

Donc (2) est un idéal maximal. On a besoin de ce résultat pour compenser le fait qu'on ait une pseudo division euclidienne comme on va le montrer maintenant.

Soit $\mathbf{I}$ un idéal non trivial de $\mathbf{A}$ et $a \in \mathbf{I}$ de norme minimale et montrons que $(a) = I$.

Soit $x \in \mathbf{I}$. Si on est dans le cas [1] de la division euclidienne alors on montre que $x \in (a)$ par minimalité de a.

Dans le cas [2], toujours par minimalité de a, $\exists q \in \mathbf{A}, 2x = aq$. Or (2) est maximal donc premier : $2 \mid q$ ou $2 \mid a$. Si $2 \mid q$, comme $\mathbf{A}$ est intègre, $a \mid x$.

Montrons que c'est le seul cas. Sinon $q \notin (2)$ et $\exists a'$ tel que $a = 2a'$. (2) est maximal et $q \notin (2)$ donc $(2, q) = \mathbf{A}$, c'est-à-dire : $\exists \lambda, \mu \in \mathbf{A}, \lambda.2 + \mu q = 1$. En multipliant par a', on obtient : $a' = \lambda a + \mu x \in \mathbf{I}$. Or $N(a') < N(a)$ ce qui est absurde. On se trouve donc toujours dans le cas $a \mid x$ c'est à dire $\mathbf{I} = (a)$ et $\mathbf{A}$ est principal.