Anneaux principaux
Exemples et applications

Dans cette leçon, les anneaux sont supposés unitaires et commutatifs et intègres

I Généralités

1) Définitions

Def : Soit A un anneau et I un idéal de A avec $I \neq A$. Alors
- I est principal si $\exists a \in A$ tel que $(a) = aA = I$
- I est premier si $\forall (a,b) \in A^2$, $ab \in I \Rightarrow a \in I$ ou $b \in I$
- I est maximal si $\forall J$ idéal de A tq $I \subset J$, alors $J = A$ ou $J = I$

Ppté : Soit I idéal de A tq $I \neq A$. Alors
- I premier $\Rightarrow A/I$ est intègre
- I maximal $\Rightarrow A/I$ est un corps.

Coro : Tout idéal maximal est premier.

Ex : Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$, $p \in \mathcal{P}$
Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{Z}$.

Def : Soit $p \in A$ et A supposé intègre. Alors, avec A^* = {inversibles} :
- p est irréductible si $p \notin A^*$ et si $p = ab \Rightarrow a \in A^*$ ou $b \in A^*$
- p est premier si $p \notin A^*$ et $p \neq 0$ et si $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$

Ppté : Tout élément premier est irréductible
Si p est premier, alors (p) est un idéal premier
Si p est irréductible, alors (p) est un idéal maximal dans l'ens des idéaux de A.

Ex : Les éléments irréductibles de $\mathbb{Z}$ sont les éléments premiers (au sens usuel)

Def : Un anneau est dit principal s'il est intègre et si tout idéal de A est principal.

Ex : $\mathbb{Z}$ est principal.

Def : Un système de représentants $\mathcal{P}$ d'irréductibles de A est un ensemble $\mathcal{P} \subset A$ d'éléments irréductibles tel que pour tout élément irréductible p de A, $\exists q \in \mathcal{P}$ tel que p et q sont associés ie $\exists u \in A^*$ tel que $p = uq$

2) Anneaux euclidiens (donc principaux)

Def : Un anneau A est dit euclidien s'il est intègre et s'il admet un stathme ie une fonction de $A \setminus \{0\} \xrightarrow{s} \mathbb{N}$ telle que si $(a,b) \in (A \setminus \{0\})^2$, $\exists (q,r) \in A^2$ tq $a = bq + r$ et ($r = 0$ ou $s(r) < s(b)$)

Th : Tout anneau euclidien est principal.

Rq : Pour I idéal, le générateur sera l'élément de stathme minimal.

Ex 1 : $\mathbb{Z}$ muni du stathme $|x|$ est euclidien.

Def : Soit A un anneau et soit $P \in A[X]$, $P \neq 0$ unitaire. Alors $\forall B \in A[X]$, on peut définir la division euclidienne par P : $\exists (Q,R) \in (A[X])^2$ tel que $B = PQ + R$ et ($R = 0$ ou $d°(R) < d°(P)$)

Rq : On peut étendre la def aux polynômes de A[X] à coeff dominant inversible (et même $\neq$ A non intègres)

Prop : Si K est un corps, alors K[X] muni du stathme $d°(P)$ est euclidien

Rq : Il y a en fait équivalence : ~~A[X] euclidien $\Leftrightarrow$ A corps~~ ; A[X] principal $\Leftrightarrow$ A corps
Donc la principalité de A ne se conserve pas

Ex 2 : K[[X]] est un anneau euclidien si K est un corps et avec le stathme ?

Ex 3 : On pose $\mathbb{Z}[i] = \{a + bi \mid (a,b) \in \mathbb{Z}^2\} \simeq \mathbb{Z}[X]/(X^2+1)$
On définit, pour $z = a + bi \in \mathbb{Z}[i]$ sa norme $N(z) = a^2 + b^2$
Alors $\mathbb{Z}[i]$ est euclidien pour le stathme N et N est multiplicative

CEx : $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est non euclidien mais principal.

Rq : Les c ex de l'implication sont durs à exhiber.

3) Anneaux factoriels (càd presque principaux)

Def : Soit A un anneau et $\mathcal{P}$ un système de représentants irréductibles de A. A est factoriel s'il est intègre et si $\forall a \in A \setminus \{0\}$, a se décompose comme $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ où $u \in A^*$, $v_p(a) \in \mathbb{N}$ où les $v_p(a)$ sont nuls sauf en nombre fini de manière unique

Rq : On appelle $\mathcal{P}$ et le choix en nombres premiers dans $\mathbb{Z}$! $\mathbb{Z}$ factoriel.

Prop : Tout anneau principal est factoriel

Cple : Soit A factoriel. Alors A vérifie
- le lemme d'Euclide : si p irréductible et $p | ab$, alors $p | a$ ou $p | b$
- le théorème de Gauss : si $a | bc$ et si $a \wedge b = 1$, alors $a | c$ (a et b sont premiers entre eux si $\forall d \neq 0$, $d | a$, $d | b$, alors $d \in A^*$)
- p irréductible $\Leftrightarrow$ p premier.

Rq / Def : Dans un anneau factoriel, on peut définir le pgcd et le ppcm de deux éléments de A (une autre def est possible) via un système de représentants : si $a = u \prod p^{v_p(a)}$ et $b = v \prod p^{v_p(b)}$, alors $a \wedge b = \prod p^{\min(v_p(a), v_p(b))}$ et $a \vee b = \prod p^{\max(v_p(a), v_p(b))}$
quoiqu'il arrive, ils sont définis à l'inversible près.

Prop / Ex : Si A est factoriel, $A[X]$ est factoriel et $A[X_1, \dots, X_n]$ aussi.
Rq : La factorialité se conserve mais c'est une prop dure !

C-Ex : $K[X,Y]$ factoriel (K corps) mais non principal.
(X, Y) est un idéal de $K[X,Y]$ qui ne s'écrit pas (P).

4) Anneaux principaux

Th de Bezout : Soit A principal et soient $a, b \in (A \setminus \{0\})^2$ ...
Alors $(a, b) = (d)$ i.e. $\exists (u, v) \in A^2$ tq $d = au + bv$

Rq : Propriété fondamentale des anneaux principaux par rapport aux anneaux factoriels.

Prop / Ex : $A[X]$ est principal ssi A est un corps

Ex 1 : $\mathbb{Z}[X]$ n'est pas principal mais $\mathbb{Q}[X]$ l'est.

Ex 2 : D, l'ensemble des décimaux est principal.

Appli : Grâce au théorème de Bezout, le calcul du pgcd via l'algorithme d'Euclide est possible

Rq : On a envie de voir les anneaux principaux si possible
- soit comme un anneau euclidien
- soit comme un anneau factoriel muni du th de Bezout

Prop : Dans A principal, I premier $\Leftrightarrow$ I maximal

C-Ex : $\mathbb{Z}[X]$ factoriel non principal :
$2\mathbb{Z}[X]$ premier mais non maximal ($\mathbb{Z}[X]/2\mathbb{Z}[X]$ pas un corps
$\bar{X}$ est non inversible !)

II Exemples et applications

1) En algèbre linéaire

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ un corps : $\mathbb{K}[X]$ donc principal et soit E un $\mathbb{K}$-ev de dim finie

Def / Prop : Soit $f \in \mathcal{L}(E)$. On définit le morphisme d'anneaux
$\varphi_f \left(\begin{array}{l} \mathbb{K}[X] \to \mathcal{L}(E) \\ P \mapsto P(f) \end{array} \right)$ et par propriété, $\mathrm{Ker}(\varphi_f) = \{P \mid P(f) = 0\}$
est un idéal de $\mathbb{K}[X]$: il est donc principal.

Donc $\exists \Pi_f \in \mathbb{K}[X]$, un polynôme annulateur de f qu'on peut choisir unitaire (car def à l'inversible près) ~~et irréductible~~
tq $(\Pi_f) = \mathrm{Ker}(\varphi_f)$. Π_f est appelé le polynôme minimal de f.

Rq : La théorie assure "seulement" l'existence de Π_f tel que $\Pi_f(f) = 0$ et si $P \in \mathbb{K}[X]$ tel $P(f) = 0$, $\Pi_f | P$.

Cro : $\mathrm{Im}(\varphi_f) = \mathbb{K}[f]$ est l'algèbre des polynômes en f.
Donc $\mathbb{K}[f] \simeq \mathbb{K}[X]/(\Pi_f)$ et $\dim(\mathbb{K}[f]) = d^\circ(\Pi_f)$

Le théorème de Bezout est crucial dans la théorie, en voici une appli

Lemme des noyaux : Soit $f \in \mathcal{L}(E)$ et $P = P_1 \dots P_k \in \mathbb{K}[X]$
$P_1, \dots, P_k$ la décomposition de P ($\forall i \neq j$, $P_i \wedge P_j = 1$). Alors
$\mathrm{Ker}\, P(f) = \mathrm{Ker}(P_1(f)) \oplus \dots \oplus \mathrm{Ker}(P_k(f))$

Def / Prop : Soit $x \in \mathbb{K}$. On définit le morphisme d'anneaux
$\varphi_x \left(\begin{array}{l} \mathbb{K}[X] \to \mathbb{K} \\ P \mapsto P(x) \end{array} \right)$ où $\mathrm{Ker}(\varphi_x)$ est un idéal principal.

Donc $\exists \Pi_x \in \mathbb{K}[X]$ un polynôme annulateur de x unitaire ~~et irréductible~~ tel que $(\Pi_x) = \mathrm{Ker}(\varphi_x)$
Π_x est appelé le polynôme minimal de x.

Prop : Π_x est irréductible (car $\mathbb{K}$ est un corps)

Def : Un endomorphisme semi-simple $f \in \mathcal{L}(E)$ est f tq pour tout sev F de E stable par f, il existe un supplémentaire de F stable par f.

DEV 1 Endomorphismes semi-simples
f est semi-simple si et ssi Π_f est sans facteurs carrés

Rq : Application du lemme des noyaux !

Appli : $M_n(\mathbb{Q})$ semi-simple dans un corps K si et ssi il existe $\bar{K}$ une extension de K dans laquelle $M_n(\mathbb{Q})$ est diagonalisable.

2) Arithmétique et corps quadratique

Rappel : $\mathbb{Z}[i]$ est un anneau euclidien muni de la norme N multiplicative

Def : Pour $p \in \mathcal{P} \setminus \{2\}$, on a $\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ carré de } \mathbb{Z}/p\mathbb{Z} \\ 0 & \text{si } p \mid x \\ -1 & \text{sinon} \end{cases}$ pour $x \in \mathbb{Z}$

DEV2 Anneau des entiers de Gauss et théorème des deux carrés

1/ - $\mathbb{Z}[i]^{\times} = \{\pm 1, \pm i\}$

2/ - $p \in \Sigma := \{n \in \mathbb{N} \mid N = a^2 + b^2, \ a, b \in \mathbb{N}\} \Leftrightarrow p = 2$ ou $p \equiv 1 [4]$

3/ - $n \in \Sigma \Leftrightarrow \forall p \equiv 3 [4], \ v_p(n)$ est pair

4/ - Les irréductibles de $\mathbb{Z}[i]$ sont aux inversibles près

- les entiers naturels premiers p tel que $p \equiv 3 [4]$
- les entiers de Gauss dont la norme est un nombre premier

Rq : La def d'irréductible se trouve dans la prochaine partie.

De manière générale, certaines équations diophantiennes sont résolues via un anneau euclidien (ou principal)

Equations diophantiennes ?

Références : PERRIN
CALAIS (Anneaux)
GOURDON
COMBES