Idéaux d'un anneau commutatif. Exemples.

$*$ = développement possible

<u>Rappel</u> : Soit A un anneau commutatif unitaire, de lois $+$ et $\times$.

$I \subset A$ est un idéal si :

- I est un sous-groupe de $(A, +)$
- $\forall x \in I, \forall a \in I, a.x \in I$.

I. Généralités

1) Propriétés faciles

- Si I et J sont des idéaux de A, alors
  - $I \cap J$ est un idéal.
  - $I + J = \{x + y \mid x \in I, y \in J\}$ est un idéal
  - $I.J = \{\sum_{\text{finie}} x_k y_k \mid x_k \in I, y_k \in J\}$ est un idéal.

$*$ Exo. Si I est un idéal, on note

$R(I) = \{x \in A \mid \exists n \in \mathbb{N}, x^n \in I\}$

Alors : $R(I)$ est idéal (radical de I).

Si I et J sont des idéaux,

$R(I.J) = R(I \cap J) = R(I) \cap R(J)$

$R(R(I)) = R(I)$; $R(I^p) = R(I)$

Si $A = \mathbb{Z}$ et $I = n\mathbb{Z}$, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

Alors $R(I) = m\mathbb{Z}$ avec $m = p_1 \cdots p_r$.

- Remarque fondamentale :

Si $I \subset A$ est un idéal, alors

$I = A \iff I$ contient un élément inversible.

- Idéaux et morphismes

Soit $f : A \to A'$ un morphisme d'anneaux.

- Si $I \subset A$ est un idéal, alors $f(I)$ est un idéal de A'
- Si $J \subset A'$ est un ideal ET si f est surjective, alors $f^{-1}(J)$ est un idéal de A.
- $\mathrm{Ker}(f)$ est un ideal de A.

2) Quotient par un idéal

Si $I \subset A$ est un idéal, alors A/I est naturellement un anneau,

$\pi : A \longrightarrow A/I$ est un morphisme surjectif d'anneaux et $\mathrm{Ker}(\pi) = I$.

Cas particulier :

Définitions : • $I \subset A$ est un idéal premier si $\forall x, y \in A$, $xy \in I \Rightarrow x \in I$ ou $y \in I$

• $I \subset A$ est un idéal maximal si pour tout idéal J vérifiant $I \subset J \subset A$, alors $J = I$ ou $J = A$.

Proposition

| I est premier $\Leftrightarrow$ A/I est intègre
| I est maximal $\Leftrightarrow$ A/I est un corps.

* Exemple $A = \mathbb{C}[X, Y]$

$I = (X)$; $J = (X, Y)$

| I est premier et A/I est isomorphe à $\mathbb{C}[Y]$
| J est maximal et A/J est isomorphe à $\mathbb{C}$.

Proposition. Soit $f : A \to A'$ un morphisme d'anneaux. Alors $A/_{\mathrm{Ker}(f)}$ est isomorphe à $\mathrm{Im}(f)$.

II Exemples fondamentaux. Applications.

1) $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$.

- Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$.
- $n\mathbb{Z}$ est premier $\Leftrightarrow$ $n\mathbb{Z}$ est maximal
  $\Leftrightarrow n \in \mathcal{P}$.

- Conséquence $\mathbb{Z}/n\mathbb{Z}$ est un corps
  $\Updownarrow$ $\mathbb{Z}/n\mathbb{Z}$ est intègre
  $\Updownarrow$ $n \in \mathcal{P}$.

Application 1 : Idéaux de $\mathbb{Z}/n\mathbb{Z}$.

Soit $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$.

Si I est un idéal de $\mathbb{Z}/n\mathbb{Z}$, alors $\pi^{-1}(I)$ est un idéal de $\mathbb{Z}$ contenant $n\mathbb{Z}$ donc de la forme $d\mathbb{Z}$ avec $d \mid n$

Si $n = dk$, alors $I = \pi(d\mathbb{Z})$
$= \{\bar{0}, \bar{d}, 2\bar{d}, \dots, (k-1)\bar{d}\}$.
est un idéal de $\mathbb{Z}/n\mathbb{Z}$,
de cardinal $k = n/d$.

Exemple $n=6$

$\mathbb{Z}/6\mathbb{Z}$ a pour idéaux
$$\begin{cases} \{\bar{0}\} & (d=6) \\ \{\bar{0}, \bar{2}, \bar{4}\} & (d=2). \\ \{\bar{0}, \bar{3}\} & (d=3) \\ \mathbb{Z}/6\mathbb{Z} & (d=1) \end{cases}$$

Application 2 pgcd et ppcm de deux entiers

Si $a, b \in \mathbb{Z}^*$, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$
$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Proposition : d est le pgcd de a et b
m est le ppcm de a et b.

2) $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps).

Thm Tout idéal non nul de $\mathbb{K}[X]$ s'écrit de façon unique $(P) = P.\mathbb{K}[X]$ où P est un polynome unitaire

De plus

$I = (P)$ est premier $\Leftrightarrow$ (P) est maximal
$\Leftrightarrow$ P est irréductible dans $\mathbb{K}[X]$.

Si c'est le cas,
$\mathbb{K}[X]/(P)$ est un corps, c'est une extension finie du corps $\mathbb{K}$, de degré égal à $\deg(P)$:

$$\dim_{\mathbb{K}} \mathbb{K}[X]/(P) = \deg(P).$$

Application 1 : Polynome minimal d'un endomorphisme d'un $\mathbb{K}$-ev E de dimension finie.

Application 2 Polynome minimal d'un

* entier algébrique.

Soit $\alpha \in \mathbb{R}$. S'il existe $P \in \mathbb{Q}[X] \setminus \{0\}$ tel que $P(\alpha) = 0$, alors

$I_\alpha = \{ P \in \mathbb{Q}[X] \mid P(\alpha) = 0 \}$ est un idéal engendré par un polynôme unitaire π_α appelé polynome minimal de α.

π_α est toujours irréductible dans $\mathbb{Q}[X]$,

$\mathbb{Q}[X]/(\pi_\alpha)$ est un corps, isomorphe à

$\mathbb{Q}(\alpha) = \mathrm{Vect}_{\mathbb{Q}}(1, \alpha, \alpha^2, \dots, \alpha^{d^\circ \pi_\alpha - 1})$ et

$\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = \deg \pi_\alpha$.

Calcul de l'inverse de $x \in \mathbb{Q}(\alpha) \setminus \{0\}$:

on écrit $x = a_0 + \dots + a_{d-1} \alpha^{d-1}$

$Q = a_0 + a_1 X + \dots + a_{d-1} X^{d-1}$ est premier avec π_α

donc $\exists\, U, V$ tels que $UQ + V\pi_\alpha = 1$

et on a $U(\alpha) Q(\alpha) = U(\alpha) x = 1$

donc $x^{-1} = U(\alpha)$.

Un <u>exercice</u> que j'<u>aime</u> bien

<u>Exercice</u> Soit $\alpha = \sqrt{2} + \sqrt{3}$

(1) Montrer que α est algébrique et déterminer π_α

* (2) Déterminer les racines de π_α dans $\mathbb{R}$.

(3) Montrer que :

$\exists A \in M_n(\mathbb{Q})$ tel que $\alpha \in Sp(A)$

$\Longleftrightarrow n \geq 4$.

3) <u>Idéaux</u> d'un <u>anneau euclidien</u>.

Un anneau <u>intègre</u> est euclidien s'il est muni d'une division euclidienne.

<u>Thm</u> Si A est euclidien, tout idéal de A est engendré par un élément, unique à un inversible près.

<u>Définition</u> Si A est un anneau intègre tel que tout idéal est engendré par un élément, alors A est principal.

Si A est principal, si $I = (x) = (y)$ alors $\exists z$ inversible dans A tel que $x = zy$.

Dans un anneau euclidien, on a

I premier $\Leftrightarrow$ I maximal

$\Leftrightarrow$ $I = (x)$ avec x irréductible dans A.

Exemples $\mathbb{Z}$, $\mathbb{K}[X]$ sont euclidiens.

Proposition. $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ est un anneau euclidien

- Si $p \in \mathcal{P}$, alors il y a équivalence entre :
  - (p) n'est pas premier dans $\mathbb{Z}[i]$
  - $p \equiv 1\ [4]$
  - $\exists a, b \in \mathbb{Z}$, $p = a^2 + b^2$.

4) PGCD dans les anneaux principaux. Théorème chinois.

Soit A un anneau (intègre) principal.

- Soient a, b deux éléments non nuls de A. Il existe d, unique à un inversible près tel que $(a) + (b) = (d)$.

  On dit que $d = \underline{pgcd(a,b)}$.

- a et b sont premiers entre eux si $pgcd(a,b) = 1$.

Théorème chinois *

Soit A un anneau intègre, $a_1, \dots, a_n$ des éléments non nuls de A, deux à deux premiers entre eux. Alors :

$$A/(a_1 a_2 \cdots a_n) \simeq A/(a_1) \times \cdots \times A/(a_n).$$

Remarque culturelle : Il existe des anneaux principaux non euclidien, le plus simple est $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$, mais il me semble difficile de proposer un développement en 15 minutes permettant de le justifier.

5) Idéaux de $\mathcal{C}([0,1],\mathbb{R})$. **

Soit $A = \mathcal{C}([0,1],\mathbb{R})$.

(1) Soit I un idéal de A. On suppose qu'il existe $f \in I$ tel que : $\forall x \in [0,1]$, $f(x) \neq 0$.

Montrer que $I = A$.

(Indic : considérer $1/f$).

(2) Soit I un idéal de A, $I \neq A$.

Soit $f_1, \dots, f_n \in I$.

Montrer qu'il existe $x \in [0,1]$ tel que $f_1(x) = \dots = f_n(x) = 0$.

(Indic : considerer $f_1^2 + \dots + f_n^2$).

(3) Soit I un idéal de A, $I \neq A$.

Le but de cette question est de montrer que :

$$\exists x \in [0,1], \ \forall f \in I, \ f(x) = 0.$$

On raisonne par l'absurde.

(a) Montrer que :

$$\forall x \in [0,1], \ \exists f_x \in I, \ \exists \delta_x > 0,$$
$$\forall y \in]x - \delta_x, x + \delta_x[, \ f_x(y) \neq 0.$$

(b) Montrer qu'il existe $x_1, \dots, x_n$ tels que

$$[0,1] \subset \bigcup_{i=1}^{n}]x_i - \delta_{x_i}, x_i + \delta_{x_i}[$$

(c) Aboutir à une contradiction en considérant $f_{x_1}, f_{x_2}, \dots, f_{x_n}$ et (2).

(4) Soit $a \in [0,1]$ et

$$M_a = \{ f \in A \mid f(a) = 0 \}$$

Montrer que M_a est un idéal maximal de A

4) (Oubli)

*

<u>Théorème</u> Soit A un anneau principal. Alors tout élément $a \in A$ se décompose en un produit $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ où les p_i sont irréductibles. La décomposition est unique à l'ordre des facteurs près et à la multiplication par un inversible près.