Algèbre 11 – Idéaux d'un anneau commutatif unitaire. Exemples et applications.

Soit A un anneau commutatif unitaire et $A^* = A \setminus \{0\}$.

1. Généralités

Définition. Une partie I de A est un *idéal* de A si I est un sous-groupe additif de A tel que $ax \in I$ pour tous $a \in A$ et $x \in I$.

Exemple. Les idéaux de $\mathbb{Z}$ sont les $a\mathbb{Z}$ avec $a \in \mathbb{N}$.

Remarque. Si I est un idéal propre de A alors $1 \notin I$; il s'ensuit que si $A \neq \{0\}$ alors A est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et A.

Proposition. *Soit $f : A \to B$ un morphisme.*

(*i*) *J idéal de $B \Rightarrow f^{-1}(J)$ idéal de A*

(*ii*) *I idéal de A et f surjectif $\Rightarrow f(I)$ idéal de B*

(*iii*) *Si f est surjectif alors $J \mapsto f^{-1}(J)$ est une bijection entre l'ensemble des idéaux de B et l'ensemble des idéaux de A contenant* $\ker f$.

Proposition. *Une intersection d'idéaux est un idéal.*

Définition. L'*idéal engendré* par une partie non vide X de A est le plus petit idéal de A contenant X *i.e.* l'intersection des idéaux de A contenant X.

Remarque. Un idéal engendré par un seul élément x est dit *principal* et noté (x) ou Ax. Un idéal engendré par un nombre fini d'éléments $x_1, \dots, x_k$ est dit *de type fini* et noté $(x_1, \dots, x_k)$ ou $Ax_1 + \cdots + Ax_k$.

Définition. L'*idéal somme* d'une famille $(I_\lambda)_{\lambda \in \Lambda}$ d'idéaux de A est l'idéal $\sum_{\lambda \in \Lambda} I_\lambda$ engendré par $\bigcup_{\lambda \in \Lambda} I_\lambda$.

Ses éléments sont les sommes finies d'éléments des I_λ.

Définition et proposition. L'*idéal produit IJ* de deux idéaux I et J de A est $\{\sum_{i=1}^{k} x_i y_i \ ; \ x_i \in I, y_i \in J\}$.

Remarque. En revanche $\{xy ; x \in I, y \in J\}$ n'est pas nécessairement un idéal de A ; prendre par exemple l'anneau $A = \mathbb{R}[X, Y]$, $I = (X)$ et $J = (Y)$.

Proposition. *Si I est un idéal de A alors le groupe quotient A/I est muni d'une structure d'anneau en posant $\overline{x} \cdot \overline{y} = \overline{xy}$.*

Définition. Soit I un idéal de A.

(*i*) On dit que I est *maximal* s'il n'existe pas d'idéal J de A tel que $I \subsetneq J \subsetneq A$.

(*ii*) On dit que I est *premier* si pour tous $x, y \in A$ tels que $xy \in A$, on a $x \in A$ ou $y \in A$.

Proposition. *Soit I un idéal de A.*

(*i*) *I maximal $\iff$ A/I corps*

(*ii*) *I premier $\iff$ A/I intègre*

Un idéal maximal est donc premier.

Exemple. $\mathbb{Z}/a\mathbb{Z}$ corps $\iff$ a est premier

Lemme de Krull. *Tout idéal de A est contenu dans un idéal maximal.*

2. Anneaux noethériens et principaux

Définition. Un *anneau principal* est un anneau intègre dont tout idéal est principal

Exemple. $\mathbb{Z}$ est un anneau principal.

Exemple. $A[X]$ principal $\iff$ A corps

Exemple. Pour que A intègre soit principal il suffit que A soit *euclidien i.e.* qu'il existe $v : A^* \to \mathbb{N}$ vérifiant

$$\forall a, b \in A^*, \exists q, r \in A / a = bq + r \text{ et } v(r) < v(b).$$

Proposition. *Tout idéal premier non nul d'un anneau principal est maximal.*

Application. Idéaux premiers de $k[X, Y]$.

Définition et proposition. On dit que A est *noethérien* si A vérifie les conditions équivalentes :

(*i*) tout idéal est de type fini,

(*ii*) toute suite croissante d'idéaux est stationnaire,

(*iii*) toute famille non vide d'idéaux admet un élément maximal.

Exemple. Un anneau principal est noethérien.

Exemple. $\mathcal{H}(\mathbb{C})$ n'est pas noethérien puisque

$$\left(\sin \frac{z}{2}\right) \subsetneq \left(\sin \frac{z}{2^2}\right) \subsetneq \cdots \subsetneq \left(\sin \frac{z}{2^n}\right) \subsetneq \cdots$$

Proposition. *A noethérien $\Rightarrow$ $A[X_1, \dots, X_n]$ noethérien*

Remarque. $A[X_1, X_2, \dots, X_n, \dots]$ n'est pas noethérien.

Corollaire. *Une algèbre de type fini sur un anneau noethérien est un anneau noethérien.*

Exemple. Un anneau d'entiers de corps de nombres est noethérien.

Exemple. $k[X^2, X^3]$ est noethérien.

Théorème de Cohen. *Si tout idéal premier de A est de type fini alors A est noethérien.*

Application. $A[[X]]$ est noethérien.

3. Divisibilité et factorisation

On suppose A est intègre de corps K.

Définition. Si $a, b \in A$ vérifient $(a) + (b) = (d)$, on dit que d est un *pgcd* de a et b.
Si $a, b \in A$ vérifient $(a) \cap (b) = (c)$, on dit que c est un *ppcm* de a et b.

Remarque. Si a et b admettent un ppcm alors ils admettent un pgcd ; par exemple, dans $\mathbb{Z}[\sqrt{-5}]$, 3 et $2 + \sqrt{-5}$ admettent 1 pour pgcd mais n'admettent pas de ppcm.

Définition et proposition. On dit que A un *anneau à pgcd* si A vérifie les conditions équivalentes suivantes

(*i*) tout couple d'éléments de A admet un pcgd,

(*ii*) tout couple d'éléments de A admet un ppcm,

(*iii*) tout élément irréductible est premier.

Définition. On dit que A est un anneau

(*i*) *atomique* si tout élément non nul non inversible se factorise en produit d'éléments irréductibles de A,

(*ii*) *factoriel* si de plus la factorisation est unique,

(*iii*) *semi-factoriel* si A est atomique et la longueur des factorisations d'un élément ne dépend que de l'élément, *i.e.* toute égalité $\pi_1 \dots \pi_r = \tau_1 \dots \tau_s$, avec les π_i, τ_j irréductibles, implique $r = s$.

Exemple. Un anneau noethérien est atomique.

Exemple. Un anneau atomique à pgcd est factoriel.

Exemple. $k[X^2, X^3]$ est atomique non semi-factoriel.

Définition. Un *idéal fractionnaire* de A est un sous-A-module de K tel qu'il existe $a \in A^*$ vérifiant $I \subset \frac{1}{a}A$.

On définit les opérations sur les idéaux fractionnaires de la même façon que pour les idéaux de A.

Définition. On dit qu'un idéal fractionnaire I est *inversible* s'il existe un idéal fractionnaire J tel que $IJ = A$; on note alors I^{-1} sont inverse.

Exemple. Si $I = Ax$ alors $I^{-1} = Ax^{-1}$.

Remarque. La multiplication d'idéaux fractionnaires est une loi de monoïde associatif d'élément neutre A.

Définition et proposition. On dit que A est un *anneau de Dedekind* si A vérifie les conditions équivalentes suivantes :

(*i*) A est intégralement clos, noethérien et tout idéal premier non nul est maximal

(*ii*) tout idéal fractionnaire de A est inversible

(*iii*) tout idéal fractionnaire I s'écrit de façon unique $I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_k^{\alpha_k}$ avec les $\mathfrak{p}_i$ premiers et $\alpha_i \in \mathbb{Z}$.

Exemple. A principal $\Rightarrow$ A de Dedekind.

Exemple. Un anneau d'entiers de corps de nombres est un anneau de Dedekind.

Définition. Le *groupe des classes d'idéaux* d'un anneau de Dedekind A est le quotient $\mathrm{Cl}(A)$ du groupe (abélien) des idéaux fractionnaires par le sous-groupe des idéaux principaux.

Proposition. *Si A est de Dedekind alors*

$$A \text{ principal} \iff A \text{ factoriel} \iff |\mathrm{Cl}(A)| = 1.$$

Lemme. *Soit $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ des idéaux premiers de A tels que $\mathfrak{p}_1 \cdots \mathfrak{p}_r = A\pi$ alors π est irréductible si et seulement s'il n'existe par de sous-produit strict $\mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_s}$ principal.*

Lemme. *Soit $\mathfrak{p}$ un idéal premier de A dont la classe $\overline{\mathfrak{p}}$ est d'ordre r dans $\mathrm{Cl}(A)$ alors on a $\mathfrak{p}^r = A\pi$ avec π irréductible.*

Théorème de Carlitz. *Soit A un anneau de Dedekind dont le groupe des classes d'idéaux $\mathrm{Cl}(A)$ est fini et tel que toute classe non nulle contienne des idéaux premiers. Alors A est semi-factoriel si et seulement si $|\mathrm{Cl}(A)| \leq 2$.*

Remarque. Les hypothèses du théorème de Carlitz sont vérifiées par les anneaux d'entiers de corps de nombres.

4. Quelques applications

4.1. **En arithmétique.**

Définition. L'*anneau des entiers de Gauss* est l'anneau $\mathbb{Z}[i]$ des entiers du corps $\mathbb{Q}(i)$ *i.e.* un entier de Gauss est un élément $z \in \mathbb{C}$ de la forme $z = a + ib$ avec $a, b \in \mathbb{Z}$.

Proposition. *$\mathbb{Z}[i]$ est un anneau euclidien dont les éléments inversibles sont $\pm 1, \pm i$.*

Proposition. *Un nombre premier $p \in \mathbb{N}$ est irréductible dans $\mathbb{Z}[i]$ si et seulement $p = a^2 + b^2$ avec $a, b \in \mathbb{N}$.*

Application. Un nombre premier $p \in \mathbb{N}$ sécrit $p = a^2 + b^2$, avec $a, b \in \mathbb{N}$, si et seulement si $p = 2$ ou $p \equiv 1 \pmod 4$.

Remarque. Si $n \geq 2$ sécrit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ alors n est somme de deux carrés si et seulement si α_i est pair dès que $p \equiv 3 \pmod 4$.

4.2. **En algèbre linéaire.** On note $k = \mathbb{R}$ ou $\mathbb{C}$ et on considère un k-espace vectoriel E de dimension finie. Si $f \in \mathcal{L}(E)$ alors l'idéal $I_f = \{P \in k[X]; P(f) = 0\}$ de $k[X]$ est principal et non réduit à $\{0\}$.

Définition. On appelle *polynôme minimal* de f le polynôme unitaire μ_f qui engendre I_f.

Proposition. *$f \in \mathcal{L}(E)$ est diagonalisable si et seulement si μ_f est scindé à racines simples.*

Définition. On dit que f est *semi-simple* si pour tout sous-espace F de E stable par f, il existe un supplémentaire S de F stable par f.

Une matrice $M \in \mathcal{M}_n(k)$ est dite semi-simple si l'endomorphisme $x \mapsto Mx$ est semi-simple.

Proposition. *f est semi-simple si et seulement si μ_f est un produit de polynôme irréductibles unitaires deux à deux distincts*

Corollaire. *Si k est algébriquement clos alors f est semi-simple si et seulement si f est diagonalisable.*

Proposition. *Soit $M \in \mathcal{M}_n(\mathbb{R})$.*

(*i*) *M est semi-simple si et seulement si M est diagonalisable dans $\mathcal{M}_n(\mathbb{C})$.*

(*ii*) *Si $M \in \mathcal{M}_n(\mathbb{R})$ est semi-simple alors il existe $P \in GL_n(\mathbb{R})$ tel que ${}^tPMP = \begin{bmatrix} D & 0 \\ 0 & B \end{bmatrix}$ avec D diagonale et B constituée de blocs de la forme $\begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}$ centrés sur sa diagonale principale.*

Développements

Idéaux premiers de $K[X, Y]$.

Théorème de Carlitz.

Endomorphismes semi-simples.

Références

[1] F. Combes, *Algèbre et géométrie*, Bréal, 1998.

[2] R. Gilmer, *Multiplicative ideal theory*, Marcel Dekker, 1972.

[3] R. Goblot, *Algèbre commutative*, Masson, 1996.

[4] X. Gourdon, *Algèbre*, Ellipses, 1994.

[5] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.