Algèbre commutative : rappels et prérequis

Dans ce document, on donne un certain nombre de définitions et de résultats plus ou moins connus sur les anneaux et les corps en général et l'anneau des polynômes à plusieurs variables en particulier.

1 Anneaux, Corps, Algèbre

1.1 Définition d'un anneau

Un anneau A est un ensemble non vide muni de deux lois internes notés $+$ et $\cdot$ telles que : $(A,+)$ est un groupe commutatif ; la loi multiplicative est associative et distributive par rapport à $+$ (i.e. $a(b+c) = ab+bc$ et $(b+c)a = ba+ca$; on demande aussi l'existence d'un neutre noté 1 pour la multiplication.
On ne demande pas que $0 \neq 1$ même si ce sera le cas en général.
On dit que A est commutatif si pour tous $a, b \in A$, $ab = ba$.
On dit que A est intègre si : $\forall a, b \in A,\ ab = 0 \Rightarrow a = 0$ ou $b = 0$.

1.2 Définition d'un corps

Un corps (commutatif) $\mathbb{K}$ est un anneau (commutatif) tel que tout élément autre que 0 admet un inverse pour la multiplication.
En particulier, un corps est un anneau intègre.
Dans toute la suite : tous les corps seront supposés commutatifs et dans un corps on exigera que $0 \neq 1$ (mais ce ne sera pas forcément le cas des anneaux).

1.3 Définition d'une algèbre

Étant donné un corps $\mathbb{K}$, une $\mathbb{K}$-algèbre A est une ensemble non vide muni de deux lois internes $+$ et $\times$ tels que :

- A est un $\mathbb{K}$-espace vectoriel,
- L'application $A \times A \to A, (a,b) \to a \times b$ est bilinéaire, i.e. pour $\lambda \in \mathbb{K}, a, b, c \in A$, on a $(\lambda a + b) \times c = \lambda a \times c + b \times c$ et idem à droite.

On parle d'algèbre associative si le produit interne $\times$ est associatif.
On parle d'algèbre commutative si le produit interne l'est.
On parle d'algèbre unitaire (ou unifère) si le produit interne possède un élément neutre.

1.4 Exemples connus

Exemples d'anneaux : $M_n(\mathbb{K})$, $\mathcal{C}([a;b],\mathbb{R})$ (ici le neutre 1 est l'application identité), $\mathbb{K}[X_1,\ldots,X_n]$.
Exemples de corps : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[i]$, $\mathbb{Z}/p\mathbb{Z}$.
Exemple d'algèbre : $M_n(\mathbb{K})$ est une $\mathbb{K}$-algèbre associative, non commutative, unitaire.

1.5 Morphismes

Étant donnés deux anneaux A et B, un morphisme d'anneaux entre A et B est une application $f : A \to B$ telle que

$$\forall x, y \in A, \quad f(x+y) = f(x) + f(y), \quad f(xy) = f(x)f(y), \quad f(1_A) = 1_B.$$

Exercice : si $f : A \to B$ est un morphisme bijectif alors f^{-1} est un morphisme d'anneaux.
Exercice : le noyau d'un morphisme d'anneau est un idéal et l'image est un sous-anneau.
Un morphisme de corps est par définition un morphisme d'anneaux entre deux corps.

Proposition. Soit $f : \mathbb{K} \to A$ un morphisme d'anneaux non nul entre un corps $\mathbb{K}$ et un anneau A, alors f est injectif.

Démonstration. Il suffit de montrer que $\ker(f)$ est trivial. Soit $x \in \ker(f)$, i.e. $f(x) = 0$. Si $x \neq 0$ alors il admet un inverse et on a alors : $f(x^{-1})f(x) = 0$ d'où $f(1_{\mathbb{K}}) = 0$ d'où $1_A = 0_A$ i.e. $A = \{0\}$ ce qui entraine que le morphisme f est nul : absurde ; par conséquent x est nul. □

1.6 Sous-corps et corps engendré

On appelle sous-corps $\mathbf{k}$ d'un corps $\mathbb{K}$ toute partie non vide de $\mathbb{K}$ qui est stable par $+$ et $\cdot$ et telle que $\mathbf{k}$ muni de ces lois est un corps.

Lemme. Soient $(\mathbf{k}_i)_{i\in I}$ une famille de sous-corps d'un corps $\mathbb{K}$. Alors l'intersection des $\mathbf{k}_i$ est un sous-corps de $\mathbb{K}$.

Démonstration. En exercice.
Question : que doit satisfaire une partie $\mathbf{k}$ de $\mathbb{K}$ pour être un sous-corps de $\mathbb{K}$? □

Définition. Soit H une partie d'un corps $\mathbb{K}$ et soit $\mathbf{k}$ un sous-corps de $\mathbb{K}$. On note $\mathbf{k}(H)$ l'intersection de tous les sous-corps de $\mathbb{K}$ qui contiennent H et $\mathbf{k}$. C'est le corps engendré par H sur $\mathbf{k}$ dans $\mathbb{K}$.
Quand H est finie, avec $H = \{\gamma_1, \dots, \gamma_p\}$, on note $\mathbf{k}(H) = \mathbf{k}(\gamma_1, \dots, \gamma_p)$.

Proposition. Soient $\mathbf{k} \subset \mathbb{K}$ deux corps et $A \subset \mathbb{K}$ alors

$$\mathbf{k}(A) = \left\{ \frac{P(a_1, \dots, a_n)}{Q(\alpha_1, \dots, \alpha_m)} \mid n, m \in \mathbb{N}; P \in \mathbf{k}[X_1, \dots, X_n],\ Q \in \mathbf{k}[X_1, \dots, X_m]; a_i, \alpha_i \in A; Q(\alpha_1, \dots, \alpha_m) \neq 0 \right\}$$

Démonstration. Notons Γ l'ensemble de droite. On montre d'abord que Γ est un corps contenant $\mathbf{k}$ et A. (stable par +, par x, par inverse)
D'où par définition de $\mathbf{k}(A)$, $\mathbf{k}(A) \subset \Gamma$. L'inclusion inverse est triviale par stabilité de $\mathbf{k}(A)$. □

Exercice. On a des choses similaires avec les algèbres.

- Une intersection de sous-algèbres est une algèbre.
- Pour une $\mathbb{K}$-algèbre unitaire A et une partie H de A, l'intersection de toutes les sous-algèbres de A contenant K (on peut voir $\mathbb{K}$ comme sous-algèbre de A si A est unitaire en identifiant λ avec $\lambda \cdot 1$) est notée $\mathbb{K}[H]$.
- On peut montrer que $\mathbb{K}[H] = \{P(h_1, \dots, h_n) \mid n \in \mathbb{N}; P \in \mathbb{K}[X_1, \dots, X_n], h_i \in H\}$

Exemple. On prend $\sqrt{2} \in \mathbb{R}$ et $\mathbb{Q} \subset \mathbb{R}$; alors le corps $\mathbb{Q}(\sqrt{2})$ est égal à l'algèbre $\mathbb{Q}[\sqrt{2}]$ elle même égale à l'ensemble $\{q + r\sqrt{2} \mid q, r \in \mathbb{Q}\}$.

1.7 Corps de fractions

On se donne un anneau A intègre (donc commutatif mais pas néssairement unitaire). On définit une relation déquivalence sur $A \times (A \setminus \{0\})$:

$$(a,b) \sim (c,d) \iff ad = bc$$

On note alors $\mathbb{K}(A)$ l'ensemble quotient.
Sur $K(A)$ on définit deux lois internes + et $\cdot$:
$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)}$,
$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac, bd)}$.

On montre alors que (exercice) :

- Les application + et $\cdot$ sont bien définies (i.e. ne dépendent pas du choix des représentants).
- L'ensemble $K(A)$ ainsi défini est un corps, appelé le corps des fractions de A.

Dans ce cas, on note simplement $\frac{a}{b}$ la classe de (a,b).

Si A est unitaire, alors l'application $A \to \mathbb{K}(A), a \mapsto \frac{a}{1}$ est un morphisme injectif d'anneaux et fait de A un sous-anneau de $K(A)$.
Si A n'est pas unitaire on considère l'application $a \to \frac{a\alpha}{\alpha}$ où α est un élément non nul fixé dans A (et on montre que ceci ne dépend pas du choix de α).
Dans les deux cas, on note $i : A \to K(A)$ cette injection.
On a alors la propriété universelle suivante :

Proposition. Étant donné un morphisme injectif d'anneaux $f : A \to \mathbb{K}$ de A vers un corps $\mathbb{K}$, il existe un unique morphisme de corps $\bar{f} : K(A) \to \mathbb{K}$ tel que $\bar{f} \circ i = f$.

Démonstration. Soit $x = a/b \in K(A)$, on définit $\bar{f}(x) = f(a)/f(b)$. On montre que c'est bien défini : si a/b = c/d, i.e. ad=bc alors $f(a)f(d) = f(b)f(c)$ dans $\mathbb{K}$ donc $f(a)/f(b) = f(c)/f(d)$ (toujours dans $\mathbb{K}$).
Ensuite c'est bien un morphisme de corps : $\bar{f}(a/b + c/d) = \bar{f}((ad+bc)/(bd)) := f(ad+bc)/f(bd) = etc$, idem pour le produit et $\bar{f}(a/a) = f(a)/f(a) = 1_{\mathbb{K}}$.
Unicité : on montre que pour un autre g tq $g \circ i = f$, on a $g(a/b) = f(a)/f(b)$. □

2 Anneaux des polynômes et idéaux

2.1 Idéal

Dans un anneau A commutatif, un idéal est une partie I non vide telle que

- I est un sous-groupe additif de A,
- pour tous $a \in A, i \in I$, $a \cdot i \in I$.

Quand l'anneau est unitaire : une partie non vide est un idéal si et seulement si pour tous $a, \in A,\ i, j \in I$, $ai \in I$ et $i + j \in I$.
On reviendra sur les idéaux dans la partie Bases de Gr.

Définition. Soit $I \subset A$ un idéal. On dit qu'il est premier si : $\forall a, b \in A, ab \in I \Rightarrow a \in I$ ou $b \in I$.
On dit qu'il est maximal si les seuls idéaux qui le contiennent sont I et A.

Exercice. 1. Si un idéal est maximal alors il est premier.

2. Soit A un anneau commutatif unitaire alors : A est un corps si et s. si ses seuls idéaux sont A et (0).
3. Dans un anneau principal, un idéal premier non nul est maximal.

Définition. Un élément $a \in A$ est dit premier s'il est non nul, non inversible et si : pour $b, c \in A$, si a divise bc alors a divise b ou c.

Exercice. — Si $a \in A$ est premier alors il est irréductible.
— La réciproque est vraie dans un anneau factoriel.
— Dans un anneau quelconque, soit $a \in A$. L'idéal $\langle a \rangle$ est premier ssi a est premier.

2.2 Caractéristique d'un corps

Étant donné un corps $\mathbb{K}$, on considère l'application $\alpha : \mathbb{Z} \to \mathbb{K}$ qui envoie n sur $n1_{\mathbb{K}}$.
Le noyau de cette application est un idéal du type $n\mathbb{Z}$ avec $n \geq 0$.

Exercice. Montrer que ce n est soit nul soit un nombre premier.

On appelle alors caractéristique de $\mathbb{K}$ cet entier.

2.3 Théorème de Krull - Lemme de Zorn

Le Lemme de Zorn, le théorème de Krull et l'axiome du choix sont trois résultats équivalents. Rappelons les.

Th. de Krull : Tout idéal $I \neq A$ d'un anneau commutatif unitaire A est inclus dans un certain idéal maximal.
C'est équivalent à : tout anneau commutatif unitaire non nul admet au moins un idéal maximal.

Lemme de Zorn : Soit $(A, \leq)$ un ensemble (partiellement) ordonné (i.e. la relation est réflexive, transitive, antisymétrique mais pas nécessairement totale : deux éléments ne sont pas forcément comparables). On suppose que A est (strictement) inductif (i.e. toute chaine admet une borne supérieure) alors A admet au moins un élément maximal.

Axiome du choix : Pour tout ensemble X d'ensembles dont aucun n'est vide, il existe une fonction définie sur X (à valeurs dans l'union de ces sous-ensembles), appelée fonction de choix, qui à chaque ensemble A appartenant à X associe un élément de cet ensemble A.

2.4 Quotient

Soit $I \subset A$ un idéal. On a une structure d'anneau sur le quotient A/I.

Proposition. On a les équivalences suivantes :
I est premier $\iff$ A/I est intègre.
I est maximal $\iff$ A/I est un corps.

Proposition. Soit $f : A \to A'$ un morphisme d'anneaux (commutatifs, unitaires) alors le noyau de f est un idéal I et f induit un morphisme d'anneaux $\bar{f} : A/I \to A'$ qui est injectif.

2.5 Anneau des polynômes

L'anneau $\mathbb{K}[X]$ est principal.
L'anneau $\mathbb{K}[X_1, \ldots, X_n]$ est factoriel.
Pour $P \in \mathbb{K}[X_1, \ldots, X_n]$, P est irréductible si et s.si $\langle P \rangle$ est un idéal premier.
Conséquence : dans $\mathbb{K}[X]$, P est irréductible si et s. si $K[X]/(P)$ est un corps.
De plus, $K[X]/(P)$ est un K-espace vectoriel de dimension le degré de P.

Définition. Soit A un anneau factoriel. Soit $P \in A[X]$.

- On dit que P est primitif si un pgcd des coefficients de P est 1.
- On définit le contenu de P, noté $\text{cont}(P)$ ou $c(P)$, comme le pgcd des coefficients de A. Il est défini à un multiple inversible près.

Proposition. Soit $P \in A[X]$ et soit $\mathbb{K} = K(A)$ son corps des fractions. Alors P est irréductible dans $A[X]$ si et s. si P est irr. dans $\mathbb{K}[X]$ et P est primitif dans $A[X]$.

Démonstration. $\Leftarrow$: On suppose $P = QR$ (le but étant de montrer que Q ou R est inversible dans $A[X]$). Si P était inversible dans $A[X]$, il le serait dans $\mathbb{K}[X]$. Alors, puisque P est irr dans $\mathbb{K}[X]$, ça implique que (par exemple) Q est inversible dans $\mathbb{K}[X]$, d'où son degré est 0. Donc $Q = c \in A$. Mais comme P est primitif, c est inversible dans A, i.e. Q est inversible dans $A[X]$.
$\Rightarrow$: P est trivialement primitif, sinon $P = cR$ avec c non inversible. Maintenant, supposons $P = QR$ avec $Q, R \in \mathbb{K}[X]$. On chasse les dénominateurs dans Q et R : $\alpha P = Q'R'$. La composante irr P apparait dans l'un des termes de droite, par exemple Q'. D'où (par intégrité de $A[X]$, on peut simplifier par P) on a $\alpha = Q''R'$. Donc R' (et donc R) est de degré nul, i.e. R est une constante i.e. R est inversible dans $\mathbb{K}[X]$. □

2.6 Critère d'Eisenstein

Soit $P = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que p divise tous les a_i sauf a_n et p^2 ne divise pas a_0. Alors P est irréductible dans $\mathbb{Q}[X]$.
Si, de plus, P est primitif alors P est irr. dans $\mathbb{Z}[X]$.

Démonstration. Supposons par l'absurde $P = QR$ avec $Q = q_n X^n + \cdots + q_0$, $R = r_m X^m + \cdots + r_0$, $P = c_d X^d + \cdots + c_0$. On regarde $\bar{P}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$ et on a : $\bar{P} = \bar{Q}\bar{R}$ ce qui donne $\overline{c_d} X^d = \bar{P}\bar{Q}$ (on est à coeff dans un corps) donc $\bar{P}$ et $\bar{Q}$ sont des monômes du type cX^e mais c'est forcément les termes de plus haut degré qui sont présents et les autres ont disparu, en particulier q_0 et p_0 sont divisible par p, ce qui entraine que a_0 est divisible par p^2. Absurde.
Pour le "de plus", on utilise la prop. précédente. □

3 Module

La notion de module est l'équivalent de celle d'espace vectoriel sur un corps $\mathbb{K}$ mais au lieu de travailler avec un corps $\mathbb{K}$, on travaille avec un anneau A. En général on voit les espaces vectoriels sur des corps commutatifs car les corps habituels (ceux qu'on voit en licence et même après) le sont. Par contre les anneaux qu'on rencontre dès la L1 (comme l'anneau des matrices) ne sont pas tous commutatifs ce qui donne lieu à une définition de module à gauche et à droite.

On se donne un anneau unitaire (non nécessairement commutatif). Un A-module à gauche M est un ensemble muni de deux lois $+$ et $\cdot$. L'ensemble M muni de $+$ est un groupe commutatif. La loi $\cdot$ est une application de $A \times M$ vers M telle que pour $a, b \in A$ et $m, n \in M$ on ait

$$a \cdot (m+n) = a \cdot m + a \cdot n \quad , \qquad (a+b) \cdot m = a \cdot m + b \cdot m \quad , \qquad (ab) \cdot m = a \cdot (b \cdot m) \quad , \qquad 1 \cdot m = m.$$

Pour définir un A-module à droite, on remplace simplement l'axiome

$$(ab) \cdot m = a \cdot (b \cdot m) \qquad \text{par} \qquad (ab) \cdot m = b \cdot (a \cdot m),$$

le reste étant inchangé.

On parle alors de sous-module. Une partie N de M est un sous-module si N est un groupe abélien pour $+$ et si pour tout $a \in A$ et $n \in N$, $a \cdot n \in N$.

On parle aussi de module de type fini et de module libre (s'il admet une base). Il faut noter que le théorème de la base incomplète est faux en général. Par exemple le $\mathbb{Z}$-module $\mathbb{Z}$ est engendré par $\{2, 3\}$ mais on ne peut pas extraire une base de cet ensemble générateur. De plus $\{2\}$ ne peut pas être complété en une base. Aussi une base n'existe pas toujours pour les modules (même en admettant l'axiome du choix). Par contre, c'est le cas si A est commutatif ou si A est noethérien (on verra cette notion plus tard) et dans ce cas on parle de dimension ou plutôt de rang du module libre.