

Résumé de cours :
Semaine 24, du 25 au 29 mars.

Barycentres et convexité

1 Barycentres (fin)

Propriété. Associativité du barycentre : Soit $k \in \mathbb{N}_p$. Notons G' le barycentre des $(A_i, \lambda_i)_{1 \leq i \leq k}$ (on suppose que $\lambda' = \sum_{i=1}^k \lambda_i \neq 0$) et G'' le barycentre des $(A_i, \lambda_i)_{k+1 \leq i \leq p}$ (on suppose que

$\lambda'' = \sum_{i=k+1}^p \lambda_i \neq 0$). Alors G est le barycentre de $((G', \lambda'), (G'', \lambda''))$.

Il faut savoir le démontrer.

Propriété. Soit $\mathcal{F}$ un sous-espace affine de $\mathcal{E}$. Si pour tout $i \in \mathbb{N}_p$, $A_i \in \mathcal{F}$, alors $G \in \mathcal{F}$.

Propriété. L'ensemble des barycentres de $A_1, \dots, A_p$ est égale à $A_1 + \text{Vect}(\overrightarrow{A_1 A_i})_{2 \leq i \leq p}$.
Il s'agit du plus petit sous-espace affine contenant $\{A_1, \dots, A_p\}$.

Exemple. Si A et B sont deux points distincts de $\mathcal{E}$, la droite (AB) est égale à l'ensemble des barycentres de A et B .

Si A, B et C sont trois points non alignés de $\mathcal{E}$, l'ensemble des barycentres de A, B et C est l'unique plan affine contenant ces trois points.

Définition. On suppose que $\mathbb{K} = \mathbb{R}$.

Une partie $\mathcal{C}$ de $\mathcal{E}$ est convexe si et seulement si elle vérifie l'une des propriétés équivalentes suivantes :

1. Pour tout $(A_1, A_2) \in \mathcal{C}^2$, $[A_1, A_2] \subset \mathcal{C}$, où $[A_1, A_2]$ est le segment d'extrémités A_1 et A_2 , c'est-à-dire l'ensemble des barycentres de $((A_1, t), (A_2, 1 - t))$, lorsque t décrit $[0, 1]$.
2. Pour tout $(A_1, A_2) \in \mathcal{C}^2$, pour tout $(\lambda_1, \lambda_2) \in \mathbb{R}_+^2 \setminus \{0\}$, le barycentre de $((A_1, \lambda_1), (A_2, \lambda_2))$ est dans $\mathcal{C}$.
3. Pour tout $p \in \mathbb{N}^*$, pour tout $(A_i)_{1 \leq i \leq p} \in \mathcal{C}^p$, pour tout $(\lambda_i)_{1 \leq i \leq p} \in \mathbb{R}_+^p \setminus \{0\}$, le barycentre de $(A_i, \lambda_i)_{1 \leq i \leq p}$ est dans $\mathcal{C}$.

Une partie est donc convexe ssi elle est stable par pour des barycentres pondérés positivement.

Exemple. Les sous-espaces affines sont des convexes.

Propriété. Une intersection de parties convexes est convexe.

Définition. Soit B une partie de $\mathcal{E}$. L'enveloppe convexe de B est le plus petit convexe de $\mathcal{E}$ contenant B . C'est l'ensemble des barycentres d'un nombre fini de points de B affectés de pondérations positives.

2 Inégalités de convexité

Notation. On fixe une application $f : I \rightarrow \mathbb{R}$, où I est un intervalle de $\mathbb{R}$ d'intérieur non vide.

Définition. f est convexe si et seulement si

$$\forall (x, y) \in I^2 \quad \forall \alpha \in [0, 1] \quad f(\alpha x + (1 - \alpha)y) \leq \alpha f(x) + (1 - \alpha)f(y).$$

f est concave si et seulement si $-f$ est convexe.

Interprétation géométrique. f est convexe si et seulement si, pour tout $x, y \in I$ avec $x < y$, le graphe de $f|_{[x, y]}$ est au dessous de la corde joignant les points $(x, f(x))$ et $(y, f(y))$.

Il faut savoir le démontrer.

Remarque. On peut également définir la stricte convexité et la stricte concavité, en remplaçant l'inégalité large par une inégalité stricte lorsque $\alpha \in]0, 1[$.

Propriété. f est concave et convexe si et seulement si elle est affine, i.e de la forme $x \mapsto \alpha x + \beta$.

Propriété. Une somme d'un nombre fini d'applications convexes est convexe.

Définition. $x_0 \in \overset{\circ}{I}$ est un point d'inflexion de f si et seulement si il existe $\varepsilon > 0$ tel que $f|_{I \cap]x_0 - \varepsilon, x_0]}$ est convexe (resp : concave) et $f|_{I \cap]x_0, x_0 + \varepsilon[}$ est concave (resp : convexe).

Propriété. L'épigraphe de f est $\{(x, y) \in \mathbb{R}^2 / x \in I \text{ et } y \geq f(x)\}$.

f est convexe si et seulement si son épigraphe est une partie convexe de $\mathbb{R}^2$.

Propriété. Inégalité de Jensen. f est convexe si et seulement si

$$\forall n \in \mathbb{N}^* \quad \forall (x_1, \dots, x_n) \in I^n \quad \forall (\lambda_1, \dots, \lambda_n) \in \mathbb{R}_+^n, \sum_{i=1}^n \lambda_i = 1 \implies f\left(\sum_{i=1}^n \lambda_i x_i\right) \leq \sum_{i=1}^n \lambda_i f(x_i).$$

Il faut savoir le démontrer.

Exercice. Si $(x_1, \dots, x_n) \in \mathbb{R}_+^n$, la moyenne géométrique $\prod_{i=1}^n x_i^{\frac{1}{n}}$ est inférieure à la moyenne

$$\text{arithmétique } \frac{1}{n} \sum_{i=1}^n x_i.$$

Il faut savoir le démontrer.

3 Croissance des pentes

Propriété. Lorsque $x, y \in I$ avec $x \neq y$, on pose $p_x(y) = \frac{f(x) - f(y)}{x - y} = p_y(x)$: c'est la pente de la corde d'extrémités $(x, f(x))$ et $(y, f(y))$. Les propriétés suivantes sont équivalentes :

1. f est convexe sur I .
2. Pour tout $a, b, c \in I$ avec $a < b < c$, $p_a(b) \leq p_a(c)$.
3. Pour tout $a, b, c \in I$ avec $a < b < c$, $p_b(a) \leq p_b(c)$.
4. Pour tout $a, b, c \in I$ avec $a < b < c$, $p_c(a) \leq p_c(b)$.

Ainsi, f est convexe si et seulement si pour tout $x_0 \in I$ l'application p_{x_0} est croissante sur $I \setminus \{x_0\}$.

Il faut savoir le démontrer.

Propriété. (Hors programme) Si f est convexe sur I , elle est dérivable à droite et à gauche en tout point de $\overset{\circ}{I}$. En particulier, elle est continue sur $\overset{\circ}{I}$.

Il faut savoir le démontrer.

4 Fonctions convexes dérivables

Propriété. Si f est dérivable, alors f est convexe si et seulement si f' est croissante.

Il faut savoir le démontrer.

Propriété. Si f est dérivable, f est convexe si et seulement si son graphe est au dessus de ses tangentes.

Il faut savoir le démontrer.

Propriété. Si f est deux fois dérivable sur I , f est convexe si et seulement si $\forall x \in I \quad f''(x) \geq 0$.

Propriété. On suppose que f est deux fois dérivable sur $\overset{\circ}{I}$ et que $x_0 \in \overset{\circ}{I}$.

Si f'' change de signe au voisinage de x_0 , alors x_0 est un point d'inflexion de f .

Les polynômes (début)

5 Le groupe des polynômes

Notation. A désigne un anneau quelconque.

Définition. On note $A[X] \triangleq A^{(\mathbb{N})}$: c'est l'ensemble des suites presque nulles.

Si $P = (a_k) \in A[X]$, on convient de noter $P = \sum_{k \in \mathbb{N}} a_k X^k$.

Remarque. Par définition, deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients.

Propriété. Si $P(X) = \sum_{k \in \mathbb{N}} a_k X^k$ et $Q(X) = \sum_{k \in \mathbb{N}} b_k X^k$, alors $P + Q = \sum_{k \in \mathbb{N}} (a_k + b_k) X^k$.

$(A[X], +)$ est un sous-groupe commutatif de $A^{\mathbb{N}}$ dont le neutre est le polynôme identiquement nul.

Définition. Si $P(X) = (a_k)_{k \in \mathbb{N}} \in A[X] \setminus \{0\}$, $\deg(P) = \max(\{k \in \mathbb{N} / a_k \neq 0\})$.

On convient que $\deg(0) = -\infty$.

Définition. Soit $P(X) = \sum_{k \in \mathbb{N}} a_k X^k \in A[X]$ un polynôme de degré $n \in \mathbb{N}$.

- a_k est le coefficient de P de degré k .
- a_0 est aussi appelé le coefficient constant du polynôme P .
- a_n est appelé le coefficient de plus haut degré de P , ou bien son coefficient dominant.
- On dit que P est unitaire (ou normalisé) si et seulement si $a_n = 1$.
- Le polynôme $a_k X^k$ est appelé un monôme.

Notation. Pour tout $n \in \mathbb{N}$, on note $A_n[X] = \{P \in A[X] / \deg(P) \leq n\}$. Ainsi, $A[X] = \bigcup_{n \in \mathbb{N}} A_n[X]$.

Propriété. $\deg(P + Q) \leq \sup(\deg(P), \deg(Q))$, avec égalité lorsque $\deg(P) \neq \deg(Q)$.

6 Produits de polynômes

Définition. $\left(\sum_{n \in \mathbb{N}} a_n X^n\right) \times \left(\sum_{n \in \mathbb{N}} b_n X^n\right) \triangleq \sum_{n \in \mathbb{N}} \left(\sum_{k=0}^n a_k b_{n-k}\right) X^n$.

Propriété. Pour tout $P, Q \in A[X]$, PQ est aussi un élément de $A[X]$.

Propriété. $(A[X], +, \times)$ est un anneau, avec $1_{A[X]} = (\delta_{k,0} 1_A)_{k \in \mathbb{N}}$.

Remarque. $\left(\sum_{n \in \mathbb{N}} a_n X^n\right) \times \left(\sum_{n \in \mathbb{N}} b_n X^n\right) \times \left(\sum_{n \in \mathbb{N}} c_n X^n\right) = \sum_{n \in \mathbb{N}} \left(\sum_{\substack{(i,j,k) \in \mathbb{N}^3 \\ i+j+k=n}} a_i b_j c_k\right) X^n$.

Propriété. L'application $i : \begin{matrix} A & \longrightarrow & A[X] \\ a & \longmapsto & (a\delta_{0,k})_{k \in \mathbb{N}} \end{matrix}$ est un morphisme injectif d'anneaux. On identifie A avec une partie de $A[X]$ en convenant que, pour tout $a \in A$, $a = i(a)$. Alors $A_0[X] = A$.

Remarque. Lorsque $b \in A$ et $P \in A[X]$, on dispose donc du produit bP .

Si $P = \sum_{k \in \mathbb{N}} a_k X^k$, on vérifie que $bP = \sum_{k \in \mathbb{N}} ba_k X^k$.

Propriété. $A[X]$ est commutatif intègre si et seulement si A est commutatif intègre.

Il faut savoir le démontrer.

Pour toute la suite de ce chapitre, on supposera que A est commutatif intègre.

Propriété. Pour tout $P, Q \in A[X]$, $\deg(PQ) = \deg(P) + \deg(Q)$.

Il faut savoir le démontrer.

Propriété. $U(A[X]) = U(A)$.

Il faut savoir le démontrer.

Définition. L'indéterminée X est le polynôme $(1_A \delta_{k,1})_{k \in \mathbb{N}}$. On a $X^n = (1_A \delta_{k,n})_{k \in \mathbb{N}}$.

7 Applications polynomiales

Définition. Soit $P = \sum_{k \in \mathbb{N}} a_k X^k \in A[X]$ un polynôme. L'application polynomiale associée à P est

l'application $\tilde{P} : \begin{matrix} A & \longrightarrow & A \\ x & \longmapsto & \sum_{k \in \mathbb{N}} a_k x^k \end{matrix}$.

Propriété. L'application $\varphi : \begin{matrix} A[X] & \longrightarrow & \mathcal{F}(A, A) \\ P & \longmapsto & \tilde{P} \end{matrix}$ est un morphisme d'anneaux.

Notation. $Im(\varphi)$ est un sous-anneau de $\mathcal{F}(A, A)$. C'est l'anneau des applications polynomiales.

Théorème. Lorsque A est un corps, φ est injectif si et seulement si A est de cardinal infini.

Algorithme d'Hörner : Soit $P = \sum_{k \in \mathbb{N}} a_k X^k \in A[X]$ et $x \in A$. On peut disposer le calcul de $\tilde{P}(x)$ de

la manière suivante : $\tilde{P}(x) = (\cdots ((a_n x + a_{n-1})x + a_{n-2}) + \cdots + a_1)x + a_0$. Cet algorithme permet de calculer $\tilde{P}(x)$ avec n multiplications et n additions.

8 Composition de polynômes

Définition. Si $P = \sum_{k=0}^n a_k X^k \in A[X]$ et $Q \in A[X]$, $P \circ Q = \sum_{k=0}^n a_k Q^k = P(Q)$.

Propriété. Pour tout $P, Q, R \in A[X]$,

- $(P + Q) \circ R = P \circ R + Q \circ R$,
- $(PQ) \circ R = (P \circ R) \times (Q \circ R)$,
- $(P \circ Q) \circ R = P \circ (Q \circ R)$.

Propriété. Soit $P, Q \in A[X]$ Si $\deg(Q) \geq 1$, alors $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Il faut savoir le démontrer.

Propriété. Pour tout $P, Q \in A[X]$, $\widetilde{P \circ Q} = \tilde{P} \circ \tilde{Q}$.

9 Dérivation formelle

Définition. Si $P = \sum_{k \in \mathbb{N}} a_k X^k \in A[X]$, on pose $P' \triangleq \sum_{k \in \mathbb{N}^*} k a_k X^{k-1} = \sum_{k \in \mathbb{N}} (k+1) a_{k+1} X^k$.

Remarque. On peut écrire $P' = \sum_{k \in \mathbb{N}} k a_k X^{k+1}$, si l'on convient que $0X^{-1} = 0$.

Définition. Si $P = \sum_{k \in \mathbb{N}} a_k X^k$, $P^{(0)} = P$ et

$$\text{pour tout } n \in \mathbb{N}, P^{(n)} = \sum_{k \geq n} \frac{k!}{(k-n)!} a_k X^{k-n} = \sum_{k \in \mathbb{N}} \frac{(k+n)!}{k!} a_{k+n} X^k.$$

Propriété. Pour tout $P \in \mathbb{R}[X]$ et $n \in \mathbb{N}$, $\widetilde{P^{(n)}} = \tilde{P}^{(n)}$.

Propriété. Pour tout $P \in A[X]$, $\deg(P') \leq \deg(P) - 1$.

Propriété. Pour tout $P \in A[X] \setminus \{0\}$, $P^{(\deg(P)+1)} = 0$.

Propriété. Soit $P, Q \in A[X]$, $a \in A$ et $n \in \mathbb{N}$.

- $(P + Q)' = P' + Q'$, et plus généralement, $(P + Q)^{(n)} = P^{(n)} + Q^{(n)}$.
- $(aP)' = aP'$, et plus généralement, $(aP)^{(n)} = aP^{(n)}$.
- $(PQ)' = P'Q + PQ'$

Propriété. Pour tout $n \in \mathbb{N}$ et $P_1, \dots, P_n \in A[X]$, $(P_1 \times \dots \times P_n)' = \sum_{i=1}^n P_i' \prod_{j \neq i} P_j$.

Formule de Leibniz : $(PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)}$.

Propriété. Pour tout $P, Q \in A[X]$, $(P \circ Q)' = Q' \times (P' \circ Q)$.

10 La structure d'algèbre de $\mathbb{K}[X]$.

Pour la suite de ce chapitre, $\mathbb{K}$ désigne un corps.

Propriété. $\mathbb{K}[X]$ est une $\mathbb{K}$ -algèbre.

Propriété. La base canonique de $\mathbb{K}[X]$ est la famille $(X^n)_{n \in \mathbb{N}}$.

Propriété. Soit $n \in \mathbb{N}$. $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ dont une base est $(1, X, \dots, X^n)$, encore appelée la base canonique de $\mathbb{K}_n[X]$. On en déduit que $\dim(\mathbb{K}_n[X]) = n + 1$.

Exercice. Soit $(P_n)_{n \in \mathbb{N}}$ une suite de polynômes de $\mathbb{K}[X]$. On suppose que cette suite de polynômes est étagée c'est-à-dire que, $\forall n \in \mathbb{N} \quad \deg(P_n) = n$.

Montrer que pour tout $N \in \mathbb{N}$, $(P_n)_{0 \leq n \leq N}$ est une base de $\mathbb{K}_N[X]$.

En déduire que $(P_n)_{n \in \mathbb{N}}$ est une base de $\mathbb{K}[X]$.

Il faut savoir le démontrer.

11 Division euclidienne entre polynômes

Théorème. Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Alors il existe un unique couple $(P, Q) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ avec $\deg(R) < \deg(B)$: Q est le quotient de la division euclidienne du dividende A par le diviseur B et que R en est le reste.

Il faut savoir le démontrer.

Définition. Soit $A \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. a est une racine de A si et seulement si $\tilde{A}(a) = 0$.

Propriété. Soit $A \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Le reste de la division euclidienne de A par $X - a$ est égal au polynôme constant $\tilde{A}(a)$.

Il faut savoir le démontrer.

Corollaire. a est racine de A si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $A = (X - a)Q$.

Propriété. Supposons que $\mathbb{L}$ est un sous-corps de $\mathbb{K}$. Alors, pour tout $(A, B) \in \mathbb{L}[X] \times (\mathbb{L}[X] \setminus \{0\})$, les quotient et reste de la division euclidienne sont les mêmes que l'on regarde A et B comme des polynômes de $\mathbb{L}[X]$ ou de $\mathbb{K}[X]$.

12 Arithmétique

12.1 Divisibilité

Définition. Soient A un anneau commutatif et $(a, b) \in A^2$. $a|b$ si et seulement si $\exists m \in A$ $b = ma$. On dit alors que a est un **diviseur** de b et que b est un **multiple** de a .

Remarque. $0|a \iff a = 0$ et, pour tout $a \in A$, $a|0$.

Propriété. Soit $P, Q \in \mathbb{K}[X]$ tels que $P \mid Q$ et $Q \neq 0$. Alors $\deg(Q) \geq \deg(P)$.

Propriété. Soit $P, Q \in \mathbb{K}[X]$ avec $Q \neq 0$. $P \mid Q$ si et seulement si le reste de la division euclidienne de P par Q est nul.

Propriété. Soit $\mathbb{L}$ un sous-corps d'un corps $\mathbb{K}$. Soit $P, Q \in \mathbb{L}[X]$.

Alors $P \mid Q$ dans $\mathbb{L}[X]$ si et seulement si $P \mid Q$ dans $\mathbb{K}[X]$.

Il faut savoir le démontrer.

Propriété. Soient A un anneau commutatif et $a, b, c, d \in A$.

- Si $b \mid a$ et $b \mid c$, alors $b \mid (a + c)$.
- Si $b \mid a$ et $d \mid c$, alors $bd \mid ac$.
- si $b \mid a$, pour tout $p \in \mathbb{N}$, $b^p \mid a^p$.

Propriété. Soient A un anneau commutatif et $b, a_1, \dots, a_p, c_1, \dots, c_p \in A$.

Si pour tout $i \in \{1, \dots, p\}$, $b \mid a_i$, alors $b \mid \sum_{i=1}^p c_i a_i$.

Propriété. Soient A un anneau commutatif et $(a, b) \in A^2$. $a|b \iff bA \subseteq aA$.

Propriété. Soit A un anneau commutatif. La relation de divisibilité est réflexive et transitive.

Définition. Soient A un anneau commutatif et $(a, b) \in A^2$.

a et b sont **associés** si et seulement si $a|b$ et $b|a$.

La relation “être associé à” est une relation d'équivalence, on la notera “ $\sim$ ”.

Propriété. Dans un anneau commutatif, si $a \sim b$ et $c \sim d$, alors $ac \sim bd$.

Hypothèse : Jusqu'à la fin de ce paragraphe, on suppose que A est intègre et commutatif.

Propriété. Soit $a, b \in A$. a et b sont associés si et seulement s'il existe $\lambda \in U(A)$ tel que $a = \lambda b$.

Il faut savoir le démontrer.

Exemple. Dans $\mathbb{Z}$, n et m sont associés si et seulement si $|n| = |m|$.

Dans $\mathbb{K}[X]$, P et Q sont associés si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$.

Propriété. La relation de divisibilité est une relation d'ordre sur $\mathbb{N}$.

La relation de divisibilité est une relation d'ordre sur l'ensemble des polynômes unitaires de $\mathbb{K}[X]$.

Définition. Soit $p \in A$. p est irréductible dans A si et seulement si $p \notin U(A)$ et si, pour tout $a, b \in A$, $p = ab \implies (a \in U(A)) \vee (b \in U(A))$.

Ainsi p est irréductible dans A si et seulement si p n'est pas inversible et a pour seuls diviseurs les éléments associés à 1 ou à p .

Remarque. Si p est irréductible, il est non nul.

Propriété. Les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés.

Exemple. Dans $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps), un polynôme P est irréductible si et seulement si il est de degré supérieur ou égal à 1 et si, pour tout $A, B \in \mathbb{K}[X]$, $P = AB \implies (\deg(A) = 0) \vee (\deg(B) = 0)$.

Remarque. Dans $\mathbb{K}[X]$:

- tout polynôme de degré 1 est irréductible ;
- tout polynôme de degré ≥ 2 possédant une racine dans $\mathbb{K}$ est réductible ;
- tout polynôme de degré 2 ou 3 sans racine dans $\mathbb{K}$ est irréductible.

Il faut savoir le démontrer.

Définition. Soit $a, b \in A$. On dit que a et b sont premiers entre eux (ou étrangers) si et seulement si les seuls diviseurs communs de a et b sont les éléments inversibles.

Définition. Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \dots, a_n \in A$.

- $a_1, \dots, a_n$ sont deux à deux premiers entre eux si et seulement si, pour tout $i, j \in \{1, \dots, n\}$ avec $i \neq j$, a_i et a_j sont premiers entre eux.
- $a_1, \dots, a_n$ sont globalement premiers entre eux si et seulement si les seuls diviseurs communs de $a_1, \dots, a_n$ sont les éléments inversibles de A .

Propriété. Soit $p \in A$ un élément irréductible et $a \in A : p|a$, ou bien p et a sont premiers entre eux.

Il faut savoir le démontrer.

12.2 PGCD

Théorème. Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est un anneau principal.

Il faut savoir le démontrer.

Notation. Jusqu'à la fin de ce chapitre "arithmétique", on fixe un anneau A que l'on suppose principal.

Définition. Soit $(a, b) \in A^2$. d est un PGCD de a et b si et seulement si $aA + bA = dA$.

Caractérisation du PGCD par divisibilité : d est un PGCD de $(a, b) \in A^2$ si et seulement si d est un diviseur commun de a et b et si, pour tout diviseur commun d' de a et b , d' divise d .

Il faut savoir le démontrer.

Propriété. a et b sont premiers entre eux si et seulement si 1 est un PGCD de a et b .

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \dots, a_k \in A$, on dit que d est un PGCD de $a_1, \dots, a_k$ si et seulement si $dA = a_1A + \dots + a_kA$, i.e si et seulement si d est un commun diviseur de $a_1, \dots, a_k$ tel que si d' est un autre commun diviseur de $a_1, \dots, a_k$, alors d' divise d .

Soit B une partie quelconque de A . d est un PGCD de B si et seulement si $dA = Id(B)$, i.e si et seulement si d est un diviseur commun des éléments de B tel que si d' est un autre diviseur commun des éléments de B , alors d' divise d .

Propriété. Lorsque $A = \mathbb{Z}$ (resp : $A = \mathbb{K}[X]$), en imposant au PGCD d'être positif (resp : unitaire) il est unique. On le note alors $a \wedge b$.

Propriété. Soit $k \in \mathbb{N}$, $a_1, \dots, a_k \in A$ et $h \in \{1, \dots, k\}$.

Alors, en convenant de noter $a \sim b$ lorsque a et b sont associés,

- Commutativité du PGCD :
pour tout $\sigma \in \mathcal{S}_k$, $PGCD(a_1, \dots, a_k) \sim PGCD(a_{\sigma(1)}, \dots, a_{\sigma(k)})$.
- Associativité du PGCD :
 $PGCD(a_1, \dots, a_k) \sim PGCD(PGCD(a_1, \dots, a_h), PGCD(a_{h+1}, \dots, a_k))$.
- Distributivité de la multiplication par rapport au PGCD : pour tout $\alpha \in A$,
 $PGCD(\alpha a_1, \dots, \alpha a_k) \sim \alpha PGCD(a_1, \dots, a_k)$.

Il faut savoir le démontrer.

12.3 PPCM

Définition. Soit $(a, b) \in A^2$. m est un PPCM de a et b si et seulement si $aA \cap bA = mA$.

Caractérisation du PPCM par divisibilité : m est un PPCM de $(a, b) \in A^2$ si et seulement si m est un multiple commun de a et b et si, pour tout multiple commun m' de a et b , m' est un multiple de m .

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \dots, a_k \in A$, m est un PPCM de $a_1, \dots, a_k$ si et seulement si $mA = a_1A \cap \dots \cap a_kA$, i.e si et seulement si m est un commun multiple de $a_1, \dots, a_k$ tel que si m' est un autre commun multiple de $a_1, \dots, a_k$, alors m' est un multiple de m .

Soit B est une partie quelconque de A . m est un PPCM de B si et seulement si $mA = \bigcap_{b \in B} bA$, i.e

si et seulement si m est un multiple commun des éléments de B tel que si m' est un autre multiple commun des éléments de B , alors m' est un multiple commun de m .

Propriété. Soit $k \in \mathbb{N}$, $a_1, \dots, a_k \in A$ et $h \in \{1, \dots, k\}$.

Alors, en convenant de noter $a \sim b$ lorsque a et b sont associés,

- Commutativité du PPCM :
pour tout $\sigma \in \mathcal{S}_k$, $PPCM(a_1, \dots, a_k) \sim PPCM(a_{\sigma(1)}, \dots, a_{\sigma(k)})$.
- Associativité du PPCM :
 $PPCM(a_1, \dots, a_k) \sim PPCM(PPCM(a_1, \dots, a_h), PPCM(a_{h+1}, \dots, a_k))$.
- Distributivité de la multiplication par rapport au PPCM :
pour tout $\alpha \in A$, $PPCM(\alpha a_1, \dots, \alpha a_k) \sim \alpha PPCM(a_1, \dots, a_k)$.