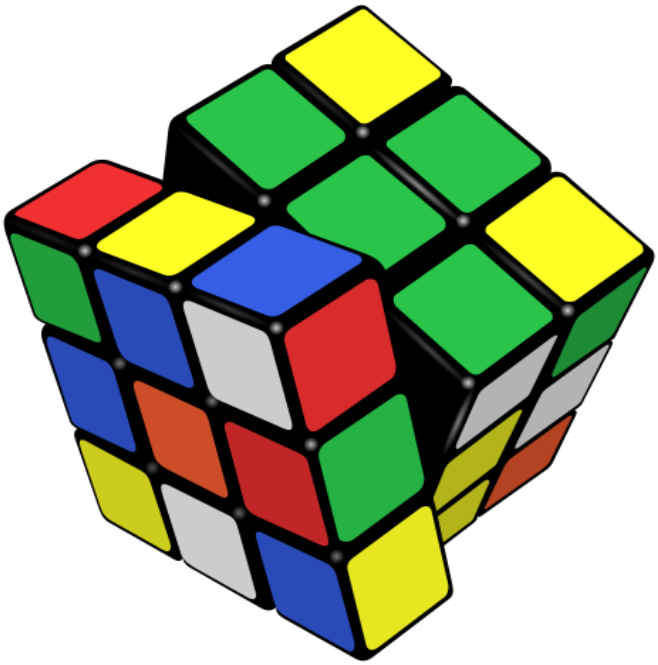
Cours de Mathématiques de MPSI:

Partie Algèbre



D'après le cours de M. Moreau, les démonstrations et exemples retirés.

CHAPITRE I : Lois de composition interne, Groupes.

1. Loi de composition interne

Définition : On appelle loi de composition interne sur un ensemble E toute application de $E \times E$ dans E notée $*$ par exemple. Elle peut avoir les qualités suivantes :

1) $*$ associativite $\Leftrightarrow \forall (x,y,z) \in E^3,\ x*(y*z) = (x*y)*z$
2) $*$ commutative $\Leftrightarrow \forall (x,y) \in E^2,\ x*y = y*x$

Définition : On appelle :

1) élément neutre de $*$ tout élément $e \in E$ tel que
$\forall x \in E,\ x*e = x = e*x.$

2) élément absorbant de $*$ tout élément $\theta \in E$ tel que
$\forall x \in E,\ x*\theta = \theta = \theta*x.$

3) élément inversible de $*$ tout élémént $x \in E$ tel que
$\exists y \in E\ /\ x*y = e = y*x$ où e est un élément neutre de $*$.

Remarque : S'il y a existence d'un élément neutre alors il y a unicité. De même si un élément est inversible et la loi associative alors il y a un unique inverse.

2. Groupes

2.1. Définition

Définition : On dit que $(G,*)$ est un groupe si il vérifie :

1) $*$ est interne sur G
2) $*$ est associative
3) $*$ admet un élément neutre dans G
4) tout élément de G est inversible pour $*$

Si $*$ est commutative sur G alors le groupe sera dit abélien ou commutatif.

Définition : Si $(G,*)$ est un groupe avec G de cardinal fini égal à n alors le groupe sera dit d'odre n.

Définition : On dit que $a \in G$ est régulier pour $*$ si et seulement si $\forall (x,y) \in G^2,\ x*a = y*a \Rightarrow x = y$ et $a*x = a*y \Rightarrow x = y$.

Propriété 1 : Si $(G,*)$ est un groupe alors tous ses éléménts sont réguliers.

Propriété 2 : $\forall (a,b) \in G^2,\ \exists! x \in G\ /\ a*x = b$.

Propriété 3 : $\forall a \in G$, les applications

$$f_a : \begin{array}{ccc} G & \to & G \\ x & \mapsto & a*x \end{array} \text{ et } g_a : \begin{array}{ccc} G & \to & G \\ x & \mapsto & x*a \end{array} \text{ sont des bijections.}$$

Propriété 4 : $\forall x \in G,\ (x^{-1})^{-1} = x$.

Propriété 5 : $\forall (x,y) \in G^2,\ (x*y)^{-1} = y^{-1} * x^{-1}$.

2.2. Sous-groupe

Définition : Soit $(G,*)$ un groupe et $H \subset G$, on dit que H est un sous-groupe de $(G,*)$ si :

1)$*$ est interne à H
2)$(H,*)$ est un groupe

Proposition : Une intersection de sous-groupes d'un groupe $(G,*)$ est un sous groupe de $(G,*)$.

2.3. Morphisme de Groupe

Définition : Soit $(G,*)$ et $(H,\diamond)$ deux groupes et une application $f : G \to H$. On dit que f est un morphisme de groupe si $\forall (x,y) \in G^2,\ f(x*y) = f(x) \diamond f(y)$.

Si f est bijective on l'appelle isomorphisme.
Si elle est de G sur G on l'appelle endomorphisme.
Un endomorphisme bijectif est appelé automorphisme.

Propriété 1 : Soit f un morphisme de $(G, *)$ dans $(H, \diamond)$ où e est l'élément neutre de $(G, *)$ et e' celui de $(H, \diamond)$ alors $f(e) = e'$.

Propriété 2 : $\forall x \in G,\ f(x^{-1}) = \Big(f(x)\Big)^{-1}$.

Propriété 3 : De plus si g est un morphisme de $(H, \diamond)$ dans un groupe $(K, \models)$ alors $g \circ f$ est un morphisme de $(G, *)$ dans $(K, \models)$.

Définition : On appelle noyau d'un morphisme f de $(G, *)$ sur $(H, \diamond)$ l'ensemble noté Ker f et définit par Ker $f = f^{-1}\left(\left\{e'\right\}\right)$ où e' est l'élément neutre de H.

Proposition : Soit f un morphisme de $(G, *)$ dans $(H, \diamond)$ alors Ker f est un sous groupe de $(G, *)$.

Théorème : Soit f un morphisme de $(G, *)$ dans $(H, \diamond)$, alors
f est injective $\Leftrightarrow$ Ker $f = \left\{e\right\}$ où e est l'élement neutre de $(G, *)$.

Définition : On appelle image d'un morphisme $(G, *)$ dans $(H, \diamond)$ l'ensemble noté Im f définit par Im $f = f(G)$.

Proposition : Im f est un sous-groupe de $(H, \diamond)$.

Remarque : f surjective $\Leftrightarrow$ Im f=H.

CHAPITRE II : Anneaux, Arithmétique et Corps.

1. Anneaux

1.1. Définition

Définition : On appelle anneau tout triplet $(A, +, \times)$ où A est un ensemble et $+$ et $\times$ sont des lois de composition internes sur A qui vérifient :

1) $(A, +)$ est un groupe abélien
2) $\times$ est associative
3) $\times$ admet un élément neutre dans A
4) $\times$ est distributive par rapport à la loi $+$

$$\Leftrightarrow \forall (a,b,c) \in A^3 \text{ on a } \begin{cases} a \times (b+c) = (a \times b) + (a \times c) \\ (a+b) \times c = (a \times c) + (b \times c) \end{cases}$$

Si la loi $\times$ y est commutative alors l'anneau sera dit commutatif.

On notera 0_A l'élément neutre de $+$ et 1_A celui de $\times$. On notera $-x$ l'opposé de $x \in A$ (inverse pour la loi $+$).

Propriété 1 : 0_A est absorbant pour $\times \Leftrightarrow \forall x \in A,\ x \times 0_A = 0_A = 0_A \times x$

Propriété 2 : $\forall (a,b) \in A^2$,

$$(-a) \times b = a \times (-b) = -(a \times b) \text{ et } (-a) \times (-b) = a \times b$$

Propriété 3 : Soient $a \in A$ et $(b_i)_{i \in \{1,\cdots,n\}} \in A^n$. Alors on a

$$a \times \left(\sum_{i=1}^{n} b_i \right) = \sum_{i=1}^{n} a \times b_i \quad \text{et} \quad \left(\sum_{i=1}^{n} b_i \right) \times a = \sum_{i=1}^{n} b_i \times a$$

Propriété 4 : Soit $(a,b) \in A^2$ tel que $a \times b = b \times a$ alors $\forall n \in \mathbb{N}^*$ on a

$$(a+b)^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} a^k \times b^{n-k}$$

$$a^n - b^n = (a-b) \times \left(\sum_{k=0}^{n-1} a^{n-1-k} \times b^k \right)$$

$$a^{2n+1} + b^{2n+1} = (a+b) \times \left(\sum_{k=0}^{2n} (-1)^k a^{2n-k} \times b^k \right)$$

1.2. Sous-anneau

Définition : Soit $(A, +, \times)$ un anneau et $B \subset A$, on dit que B est un sous-anneau de $(A, +, \times)$ si :

1) $(B, +)$ est un sous-groupe de $(A, +)$
2) B est stable par $\times$
3) $1_A \in B$

et alors $(B, +, \times)$ sera aussi un anneau.

1.3. Morphisme d'anneaux

Définition : Soient $(A, +, \times)$ et $(B, \oplus, \otimes)$ deux anneaux et $f : A \to B$.

$$f \text{ morphisme d'anneaux} \Leftrightarrow \begin{cases} \forall (a,b) \in A^2,\ f(a+b) = f(a) \oplus f(b) \\ \forall (a,b) \in A^2,\ f(a \times b) = f(a) \otimes f(b) \\ f(1_A) = 1_B \end{cases}$$

2. Arithmétique

2.1. Anneaux $(\mathbb{Z}, +, \times)$ et division euclidienne

Proposition : $(\mathbb{Z}, +, \times)$ est un anneau muni d'une relation d'ordre total $\leqslant$ compatible avec $+$, tel que toute partie non vide majorée (respectivement minorée) de $\mathbb{Z}$ admet un plus grand élément (respectivement plus petit).

Propriété : $\mathbb{Z}$ est archimédien $\Leftrightarrow \forall x \in \mathbb{N}^*,\ \forall y \in \mathbb{Z},\ \exists n \in \mathbb{N} \ /\ nx > y$.

Théorème de la division euclidienne :

$$\forall (a,b) \in \mathbb{Z} \times \mathbb{N}^*,\ \exists! (q,r) \in \mathbb{Z} \times \mathbb{N} \text{ tel que } \begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$$

Conséquence : Les seuls sous-groupes de $(\mathbb{Z}, +)$ sont les parties de la forme $n\mathbb{Z}$ avec $n \in \mathbb{Z}$.

Définition : Soit A un sous-groupe non réduit à $\Big\{0\Big\}$ de $(\mathbb{Z}, +)$, on appelle

générateur de A son plus petit élément n non nul et positif, il est tel que $A = n\mathbb{Z}$.

2.2. Divisibilité

Définition : On appelle relation de divisibilité notée $|$ sur $(\mathbb{Z}, +, \times)$, la relation binaire définie par : $\forall (a, b) \in \mathbb{Z}^2,\ a|b \Leftrightarrow \exists c \in \mathbb{Z}\ /\ b = ac$.

Proposition : La relation $|$ est réfléxive, transitive mais non antisymétrique.

Définition : Comme $|$ est non antisymétrique, il sera dit de $(a, b) \in \mathbb{Z}^2$ tel que $a|b$ et $b|a$ qu'ils sont associées (car non nécessairement égaux).

Proposition : Soient $(a, b) \in \mathbb{Z}^2$ tel que a et b soient associées, alors $a = b$ ou $a = -b$.

Proposition : $\forall (a, b) \in \mathbb{Z}^2, a|b \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$.

Remarque : Dans $\mathbb{N}^*, a|b \Rightarrow a \leqslant b$.

Proposition : Soient $(a, b) \in (\mathbb{Z}^*)^2$, soit $H(a, b) = a\mathbb{Z}+b\mathbb{Z} = \Big\{c \in \mathbb{Z}\ /\ \exists (u, v) \in \mathbb{Z}^2, c = au + bv\Big\}$, alors $H(a, b)$ est un sous-groupe de $(\mathbb{Z}, +)$ non réduit à $\Big\{0\Big\}$.

2.3. PGCD

Définition : Soit $(a, b) \in (\mathbb{Z}^*)^2$, on appelle PGCD de a et de b le générateur du sous-groupe $a\mathbb{Z} + b\mathbb{Z}$. On le notera $PGCD(a, b)$ ou encore $a \wedge b$.

Proposition : Soit $(a, b, d) \in (\mathbb{Z}^*)^3$, $d|a$ et $d|b \Rightarrow d|a \wedge b$.

Proposition : Soit $(a, b) \in (\mathbb{Z}^*)^2$, $a \wedge b$ est le plus grand des entiers positifs divisant a et b.

Remarque : Soit $a \in \mathbb{Z}^*$, alors $a \wedge a = |a|$. Et pour tout b on a $a \wedge b = b \wedge a$.

Proposition : Soit $(a, b) \in (\mathbb{Z}^*)^2$, $a \wedge b = |a| \Leftrightarrow a|b$.

Proposition : Soit $(a, b, c) \in (\mathbb{Z}^*)^3,\ (ab) \wedge (ac) = |a|(b \wedge c)$.

Proposition : Soit $(a, b, d) \in (\mathbb{Z}^*)^2 \times \mathbb{N}^*$ tel que $d|a$ et $d|b$ alors $\exists (a', b') \in (\mathbb{Z}^*)^2 \ / \ a = a'd$ et $b = b'd$. On a alors $d = a \wedge b \Leftrightarrow a' \wedge b' = 1$.

2.4. PPCM

Proposition : Soit $(a, b) \in (\mathbb{Z}^*)^2$, $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ non réduit à $\Big\{0\Big\}$.

Définition : Soit $(a, b) \in (\mathbb{Z}^*)^2$, on appelle PPCM de a et de b le générateur de $a\mathbb{Z} \cap b\mathbb{Z}$. On le notera $PPCM(a, b)$ ou alors $a \vee b$.

Remarque : $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

Proposition : $a \vee b$ est le plus petit des entiers positifs multiples communs à a et b.

Proposition : Soit $(a, b, c) \in (\mathbb{Z}^*)^3$ alors $a|c$ et $b|c \ \Rightarrow a \vee b|c$.

Proposition : Soit $(a, b) \in (\mathbb{Z}^*)^2$:

1) $a \vee b = b \vee a$
2) $a \vee b = |a| \vee |b|$
3) $a \vee a = |a|$
4) $a \vee 1 = |a|$
5) $a \vee b = |b| \Leftrightarrow a|b$

Proposition : Soit $(a, b, c) \in (\mathbb{Z}^*)^3$, $(ab) \vee (ac) = |a|(b \vee c)$.

Théorème : Soit $(a, b) \in (\mathbb{Z}^*)^2$, $(a \vee b)(a \wedge b) = |ab|$.

2.5. Nombres premiers entre eux

Définition : On dit que a et b sont premiers entre eux si et seulement si $a \wedge b = 1$.

Théorème de Bézout : Soit $(a, b) \in (\mathbb{Z}^*)^2$,

$$a \wedge b = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z} \ / \ au + bv = 1.$$

Corollaire : Soit $(a, b, c) \in (\mathbb{Z}^*)^3$

1) $a \wedge (bc) = 1 \Leftrightarrow a \wedge b = 1$ et $a \wedge c = 1$
2) $a \wedge b = 1 \Rightarrow \forall (m, n) \in (\mathbb{N}^*)^2,\ a^m \wedge b^n = 1.$
3) $a \wedge b = 1 \Rightarrow a \wedge bc = a \wedge c.$

Théorème de Gauss : Soit $(a, b, c) \in (\mathbb{Z}^*)^3$, $a|bc$ et $a \wedge b = 1 \ \Rightarrow a|c.$

Corollaire : Soit$(a, b, n) \in (\mathbb{Z}^*)^3$, si $a \wedge b = 1,\ a|n$ et $b|n$ alors $ab|n.$

Théorème d'Euclide : Soit $(a, b, q, r) \in (\mathbb{Z}^*)^4$ tel que $a = bq + r$ alors $a \wedge b = b \wedge r$

Recherche du PGCD de deux entiers : On suppose que $(a, b) \in (\mathbb{N}^*)^2$, car on sait que $a \wedge b = |a| \wedge |b|$. Et on suppose aussi $a \geqslant b$. On effectue la division euclidienne de a par b, alors on obtient $a = bq + r$ et $0 \leqslant r < b$, mais aussi $a \wedge b = b \wedge r$. Si $r = 0$ alors le $PGCD$ est b, sinon on recommence le procédé avec b et r, on obtient donc une suite strictement décroissante de restes dont le dernier non nul est le $PGCD$ de a et de b.

2.6. Nombres premiers

Définition : On appelle nombre premier tout nombre entier $p \in \mathbb{N}\backslash\{0, 1\}$ qui ne soit divisible que par 1 et par lui-même.

Propriété 1 : Tout nombre premier est premier avec tout entier qu'il ne divise pas.

Propriété 2 : Deux nombres premiers distincts sont premiers entre eux.

Propriété 3 : Soit p premier et $(a, b) \in (\mathbb{Z}^*)^2$ alors $p|ab \Rightarrow p|a$ ou $p|b$.

Propriété 4 : Tout entier $n \leqslant 2$ admet au moins un diviseur premier.

Propriété 5 : L'ensemble $\mathcal{P}$ des nombres premiers est infini.

2.7. Factorisation en nombres premiers

Définition : Soit $n \geqslant 1$ et p premier. On appelle p-valuation de n le plus grand entier α tel que $p^\alpha|n$, et on le note $V_p(n)$. De plus on appelle support

premier de n l'ensemble des nombres premiers p tels que $V_p(n) \geqslant 1$ et l'on note cet ensemble $V_p(n)$.

Théorème : Soient n un entier, $(p_1, \cdots, p_m) \in \mathcal{P}^m$ distincts, et $(\alpha_1, \cdots, \alpha_m) \in \mathbb{N}^m$ tels que $p_1^{\alpha_1}|n, \cdots, p_m^{\alpha_m}|n$ alors $\prod_{i=1}^{m} p_i^{\alpha_i}|n$.

Théorème de la décomposition : $\forall n \geqslant 1,\ n = \prod_{p \in \mathcal{P}(n)} p^{V_p(n)}$ et cette décomposition en produit de facteur premier est unique.

3. Corps

3.1. Définition

Définition : On dit que $(K, +, \times)$ est un corps si :

1) $(K, +, \times)$ est un anneau commutatif
2) $(K\backslash\{0\}, \times)$ est un groupe commutatif.

Remarque : $(K, +\times)$ est un corps $\Rightarrow K \neq \{0_K\}$ donc $1_K \neq 0_K$.

3.2. Sous-corps

Définition : On dit que $H \subset K$ est un sous-corps du corps $(K, +, \times)$ si :

1) H est un sous anneau de $(K, +, \times)$
2) $\forall h \in H\backslash\{0\},\ h^{-1} \in H$

Remarque : Un sous-corps est un corps, et tous les corps sont commutatifs.

CHAPITRE III : Algèbre linéaire

1. Espace vectoriel sur un corps K

1.1. Définition

Définition : On dit que E est un K-espace vectoriel, où K est un corps, si :

1) E est muni d'une loi notée $+$ de composition interne tel que $(E,+)$ soit un groupe commutatif

2) E est muni d'une loi externe notée $\cdot$, c'est à dire d'une application de $K \times E \to E$ qui vérifie :

$$(i)\ \forall u \in E,\ 1_K.u = u$$
$$(ii)\ \forall \lambda \in K, \forall (u,v) \in E^2,\ \lambda.(u+v) = \lambda.u + \lambda.v$$
$$(iii)\ \forall (\lambda,\mu) \in K^2,\ \forall u \in E,\ (\lambda+\mu).u = \lambda.u + \mu.u$$
$$(iv)\ \forall (\lambda,\mu) \in K^2,\ \forall u \in E,\ \lambda.(\mu.u) = (\lambda \times \mu).u$$

Les éléments de E sont appelés les vecteurs, ceux de K les scalaires. L'élément neutre de $(E,+)$ sera noté $\overrightarrow{0}$. Le vecteur opposé d'un vecteur u sera noté $-u$.

Propriété 1 : $\forall u \in E,\ 0_K.u = \overrightarrow{0}$

Propriété 2 : $\forall \lambda \in K,\ \lambda.\overrightarrow{0} = \overrightarrow{0}$

Propriété 3 : $\forall \lambda \in K,\ \forall u \in E,\ \lambda.u = \overrightarrow{0} \Rightarrow \lambda = 0$ ou $u = \overrightarrow{0}$

Propriété 4 : $\forall \lambda \in K,\ \forall u \in E,\ (-\lambda).u = \lambda.(-u) = -(\lambda.u)$

1.2. Structure d'espace vectoriel produit

Définition : Soient E et F deux K-espace vectoriels. On définit sur $E \times F$ une loi $+$ par $(u,v)+(u',v') = (u+u', v+v')$. Alors $(E \times F, +)$ est un groupe commutatif tel que $0_{E\times F} = (0_E, 0_F)$ et $-(u,v) = (-u,-v)$. De même on définit une loi externe $\cdot$ sur $E \times F$ définie par $\lambda.(u,v) = (\lambda.u, \lambda.v)$. Et alors muni de ces deux lois, $(E \times F, +, \cdot)$ est un K espace vectoriel.

On peut généraliser à n K-espaces vectoriels, $E_1, \cdots, E_n$. On peut définir

sur $E = E_1 \times E_2 \times \cdots \times E_n$ une loi interne $+$ et une loi externe $\cdot$ relativement à ce qui précède, tel que $(E, +, \times)$ soit un K-espace vectoriel.

1.3. Sous-espace vectoriel

Définition : Soit E un K-espace vectoriel et $F \subset E$. On dit que F est un sous-espace vectoriel de E si :

1) F est un sous-groupe de $(E, +)$
2) F est stable par la loi externe

De manière équivalente si :

1) $F \neq \emptyset$
2) F stable par $+$
3) F stable par $\cdot$

On peut réunir 2) et 3) en F est stable par combinaison linéaire :

$$\forall(\lambda, \mu) \in K^2,\ \forall(x, y) \in F^2,\ \lambda.x + \mu.y \in F$$

Un sous-espace vectoriel est un espace vectoriel, et $\left\{ \overrightarrow{0} \right\}$ est un sous-espace vectoriel.

1.4. Intersection de sous-espace vectoriel

Proposition : Toute intersection de sous-espaces vectoriels d'un K-espace vectoriel E est un sous-espace vectoriel de E.

Définition : Soit $A \subset E$ où E est un espace vectoriel, on appelle sous-espace vectoriel engendré par A l'intersection de tous les sous-espaces vectoriels contenant A, et on le note $Vect(A)$. Et alors $Vect(A)$ est le plus petit sous-espace vectoriel contenant A pour la relation $\subset$.

1.5. Somme de sous-espace vectoriel

Définition : Soit F et G deux sous-espaces vectoriel d'un même K-espace vectoriel E. On appelle somme de F et G notée $F + G$ la partie $F + G = \left\{ w \in E \ / \ \exists(u, v) \in F \times G,\ w = u + v \right\}$.

Proposition : $F + G$ est un sous-espace vectoriel de E.

Définition : On dit que la somme $F + G$ est directe si $F \cap G = \left\{\overrightarrow{0}\right\}$. Elle sera alors notée $F \oplus G$.

Définition : On dit que deux sous-espaces vectoriels F et G d'un K-espace vectoriel E sont supplémentaire si $\forall w \in E,\ \exists!(u, v) \in F \times G\ /\ w = u + v$.

Proposition : F et G supplémentaires $\Leftrightarrow F \oplus G = E$.

2. Sous-espace affine d'un K-espace vectoriel

2.1. Translations

Définition : Soit E un K-espace vectoriel et $u \in E$, on appelle translation de vecteur u l'application $t_u : \begin{array}{ccc} E & \to & E \\ v & \mapsto & v + u \end{array}$. On note $T(E)$ l'ensemble des translations de E, alors $(T(E), \circ)$ est un groupe commutatif isomorphe au groupe $(E, +)$.

2.2. Sous-espaces affines

Définition : Soit E un K-espace vectoriel, on appelle sous-espace affine passant par $a \in E$ et de direction le sous-espace vectoriel F l'ensemble des vecteurs de la forme $a + u$ où $\in F$. On le note $a + F$.

Propriété 1 : Soient F un sous-espace vectoriel de E, et $(a, b) \in E^2$,

$$b \in a + F \Leftrightarrow \exists v \in F\ /\ b = a + v.$$

Propriété 2 : Soit $a \in E$ alors $a + \left\{\overrightarrow{0}\right\} = \left\{a\right\}$.

Propriété 3 : Soient F un sous-espace vectoriel de E, et $(a, u) \in E^2$,

$$a + u \in a + F \Leftrightarrow u \in F.$$

Propriété 4 : Soient F un sous-espace vectoriel de E, et $a \in E$,

$$a + F = F \Leftrightarrow a \in F.$$

Propriété 5 : Soient F et G deux sous-espaces vectoriels de E, $(a, b) \in E^2$,

$$a + F \subset b + G \Leftrightarrow F \subset G \text{ et } b - a \in G.$$

Propriété 6 : $a + F = b + G \Leftrightarrow F = G$ et $b - a \in F$ (respectivement G).

Propriété 7 : $a + F = b + F \Leftrightarrow b - a \in F$

Propriété 8 : $a + F = a + G \Leftrightarrow F = G$

Définition : On dit que le sous-espace affine $a + F$ est parralèle au sous-espace affine $b + G$ si $F \subset G$.

Proposition : L'intersection des deux sous-espaces affines $a + F$ et $b + G$ est soit vide soit un sous-espace affine de direction $F \cap G$.

Définition : On dit que $a + F$ et $b + G$ sont supplémentaires si F et G sont supplémentaires.

Théorème : L'intersection de deux sous-espaces affines supplémentaires est réduite à un point.

Remarque : Tout vecteur d'un K-espace vectoriel peut-être vu comme un point. A deux points a et b de E on associe le vecteur $\overrightarrow{ab} = b - a$. La droite affine passant par a et b est donc le sous-espace affine passant par a et de direction $K.\overrightarrow{ab}$ donc $a + K.\overrightarrow{ab}$.

Théorème : Soient $(a_1, \cdots, a_n) \in E^n$ où E est un K-espace vecoriel et $(\alpha_1, \cdots, \alpha_n) \in K^n$. Soit $f : u \mapsto \sum_{i=1}^{n} \alpha_i.\overrightarrow{ua_i}$ et $\alpha = \sum_{i=1}^{n} \alpha_i$.
1) si $\alpha = 0$, f est constante sur E.
2) si $\alpha \neq 0$, alors f est bijective. Et on appelle barycentre des points a_i pondérés des coefficients α_i l'unique point $g \in E$ tel que $f(g) = \overrightarrow{0}$.

3. Application linéaire

3.1. Définition

Définition : On appelle application linéaire du K-espace vectoriel E dans le K-espace vectoriel F toute application $f : E \to F$ telle que :

1) $\forall (u,v) \in E^2,\ f(u+v) = f(u) + f(v)$
2) $\forall \lambda \in K,\ \forall u \in E,\ f(\lambda.u) = \lambda.f(u)$

Ce qui peut se regrouper en,

$$\forall (u,v) \in E^2,\ \forall \lambda \in K,\ f(u + \lambda.v) = f(u) + \lambda.f(v)$$

On peut voir comme conséquence directe de la définition que $f(\overrightarrow{0}_E) = \overrightarrow{0}_F$ car f est un morphisme du groupe $(E,+)$ vers le groupe $(F,+)$.

Définition : Une application linéaire d'un K-espace vectoriel E dans K (car on sait que tout corps K peut-être vu comme K-espace vectoriel) est appelée forme linéaire.

Une application linéaire de E dans E est appelée endormorphisme de E.

Une application linéaire bijective de E sur F est appelée isomorphisme de E sur F.

Un endomorphisme bijectif de E est appelée automorphisme de E.

3.2. Espace vectoriel $\mathcal{L}(E,F)$

Définition : On appelle $\mathcal{L}(E,F)$ l'ensemble formépar les applications linéaires de E sur F. On définit sur $\mathcal{L}(E,F)$ une loi + par :

$\forall (f,g) \in (\mathcal{L}(E,F))^2,\ f+g : \begin{array}{ccc} E & \to & F \\ u & \mapsto & f(u)+g(u) \end{array}$

De même on définit une loi externe $\cdot$ par :

$\forall \lambda \in K,\ \forall f \in \mathcal{L}(E,F),\ \lambda.f : \begin{array}{ccc} E & \to & F \\ u & \mapsto & \lambda.f(u) \end{array}$

Théorème : $\mathcal{L}(E,F)$ muni de la loi interne + et de la loi externe $\cdot$ est un K-espace vectoriel.

Définition : On notera l'ensemble des endomorphismes de E de la manière suivante $\mathcal{L}(E)$ au lieu de $\mathcal{L}(E,E)$.

3.3. Composition d'applications linéaires

Proposition : Soit $f \in \mathcal{L}(E,F)$ et $g \in \mathcal{L}(F,G)$ où E, F, et G sont trois K-espaces vectoriels. Alors $g \circ f \in \mathcal{L}(E,G)$.

Proprosition : Soient E, F et G trois K-espaces vectoriels et $f \in \mathcal{L}(E,F)$ alors l'application $\varphi : \begin{array}{ccc} \mathcal{L}(F,G) & \to & \mathcal{L}(E,G) \\ g & \mapsto & g \circ f \end{array}$ est une application linéaire de $\mathcal{L}\Big(\mathcal{L}(F,G), \mathcal{L}(E,G)\Big)$.

De même soit $g \in \mathcal{L}(F,G)$ alors l'application $\psi : \begin{array}{ccc} \mathcal{L}(E,F) & \to & \mathcal{L}(E,G) \\ f & \mapsto & g \circ f \end{array}$ est une application linéaire de $\mathcal{L}\Big(\mathcal{L}(E,F), \mathcal{L}(E,G)\Big)$.

Proposition : $(\mathcal{L}(E), \circ)$ est un anneau non commutatif.

3.4. Noyau et image d'une application linéaire

Définition : Soit $f \in \mathcal{L}(E,F)$ alors on appelle noyau de f l'ensemble $\ker f = f^{-1}\left(\left\{\overrightarrow{0}\right\}\right)$ et on appelle l'image de f l'ensemble $\text{Im } f = f(E)$.

Proposition : Soit $f \in \mathcal{L}(E,F)$ alors $\ker f$ est un sous-espace vectoriel de E et $\text{Im } f$ est un sous-espace vectoriel de F.

Proposition : Soit H un sous-espace vectoriel de E, et $f \in \mathcal{L}(E,F)$ alors $f(H)$ est un sous espace vectoriel de F.

3.5. Equation linéaire

Définition : On appelle équation linéaire toute équation de la forme $f(u) = v$ où $f \in \mathcal{L}(E,F)$, $v \in F$ et d'inconnue $u \in E$. Résoudre l'équation revient à déterminer $S = f^{-1}\left(\left\{v\right\}\right)$.

1^{er} cas : $S = \emptyset$ alors l'équation n'a pas de solution.

2^{nd} cas : $S \neq \emptyset$. Alors S admet au moins une solution u_0 et alors S est le sous-espace affine $S = u_0 + \ker f$.

3.6. Projecteurs

Définition : On appelle projecteur du K-espace vectoriel E tout endomorphisme p de E tel que $p \circ p = p$.

Proposition : Soit F et G deux sous-espaces vectoriels de E supplémentaires.

Alors l'application f de E dans F qui à tout vecteur $w \in E$ se décomposant $w = u + v$ où $u \in F$ et $v \in G$ associe le vecteur $f(w) = u$ est un projecteur de E appelé projecteur sur F parralèlement à G.

Théorème : Soit p un projecteur de E alors p projette sur Im p parallèlement à ker p.

Proposition : Soit p le projecteur sur F parallèlement à G, et q le projecteur sur G parallèlment à F alors $q = Id_E - p$ ce qui nous donne Im $p =$ ker $(Id_E - p)$ et ker $p = \text{Im}(Id - q)$.

3.7. Application réciproque d'un endormorphisme

Théorème : Soit f un isomorphisme du K-espace vectoriel E sur le K-espace vectoriel F. Alors f^{-1} est un isomorphisme de F sur E.

3.8. Affinités vectorielles

Définition : Soit F et G deux sous-espaces vectoriels supplémentaires du K-espace vectoriel E. On appelle affinité de rapport $\lambda \in K$, d'axe F et de direction G l'application $f : E \to E$ qui à tout vecteur $w = u + v$ avec $u \in F$ et $v \in G$ associe $f(w) = u + \lambda.v$ On remarque que si $\lambda = 0_K$ alors cette affinité effectue en réalité une projection sur son axe parallèlement à sa direction.

3.9. Symétries vectorielles et involutions linéaires

Définition : Soient F et G deux-sous espaces vectoriels supplémentaires du K-espace vectoriel E. On appelle symétrie vectorielle d'axe F et de direction G l'afffinité vectorielle de rapport $\lambda = -1_K$.
On appelle involution de E tout application $f : E \to E$ vérifiant $f \circ f = Id_E$. Toute involution est donc bijective et vérifie donc $f^{-1} = f$.

Théorème : Soit f un endomorphisme de E alors :

$$f \text{ symétrie vectorielle de } E \Leftrightarrow \ f \text{ involution linéaire de } E.$$

3.10. Groupe linéaire $GL(E)$

Définition : On appelle $GL(E)$ l'ensemble des automorphisme de E.

Théorème : $(GL(E), \circ)$ est un groupe non commutatif.

CHAPITRE IV : Polynômes

1. $\mathbb{K}$-Espace vectoriel des polynômes

1.1. Définition

Définition : On appelle polyôme à coefficients dans le corps infini $\mathbb{K}$ toute suite $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ presque nulle, c'est à dire $\exists p_0 \in \mathbb{N}$ / $\forall n \geq p_0,\ a_n = 0$.

Définition : L'ensemble des polynômes sur $\mathbb{K}$ est noté $\mathbb{K}[X]$. Le polynôme $(0, 0, 0, \cdots)$ est appelé polynôme nul noté 0 et $(1, 0, 0, \cdots)$ polynôme unité noté 1.
Définition : Soit $P \in \mathbb{K}[X]$, si $P \neq 0$, soit $A = \left\{n \in \mathbb{N} \ / \ a_n \neq 0\right\}$, A admet un plus grand élément qu'on appelle degré de P noté deg P et $a_{\deg\ P}$ est appelé coefficient dominant. Si $a_{\deg\ P} = 1$, P est dit unitaire. Par définition deg $0 = -\infty$.

Proposition : Soit $(P, Q) \in (\mathbb{K}[X])^2$, avec $P = (a_n)$ et $Q = (b_n)$,

$$P = Q \Leftrightarrow \forall n \in \mathbb{N},\ a_n = b_n.$$

1.2 Addition des polynômes

Définition : On définit sur $\mathbb{K}[X]$ la loi + par restriction de l'addition des suites aux polynômes. Soit $(P, Q) \in (\mathbb{K}[X])^2$, avec $P = (a_n)$ et $Q = (b_n)$, alors $P + Q = (a_n + b_n)$. Si on a p_0 et q_0 tels que $\forall n \geq p_0,\ a_n = 0$ et $\forall n \geq q_0,\ b_n = 0$ donc $\forall n \geq \max(p_0, q_0),\ a_n + b_n = 0$, donc $P + Q$ est bien un polynôme.

Propriété 1 : $\forall (P, Q) \in (\mathbb{K}[X])^2$, $\deg(P + Q) \leq \max(\deg\ P, \deg\ Q)$.

Propriété 2 : Soit $(P, Q) \in (\mathbb{K}[X])^2$, si $\deg P \neq \deg Q$, alors $\deg(P+Q) = \max(\deg P, \deg Q)$.

Propriété 3 : $(\mathbb{K}[X], \circ)$ est un groupe commutatif.

1.3. Multiplication des polynômes

Définition : On définit sur $\mathbb{K}[X]$ une miltiplication $\times$ par $\forall (P,Q) \in (\mathbb{K}[X])^2$, avec $P_(a_n)$ et $Q = (b_n)$ alors on définit $P \times Q = (c_n)$ par $c_n = \sum_{i=0}^{n} a_k b_{n-k}$.

Propriété 1 : $\times$ est interne à $\mathbb{K}[X]$.

Propriété 2 : $\times$ est commutative sur $\mathbb{K}[X]$.

Propriété 3 : $\times$ est associative sur $\mathbb{K}[X]$.

Propriété 4 : $\times$ est distributive par rapport à la loi $+$.

Propriété 5 : $\times$ admet un élément neutre dans $\mathbb{K}[X]$ qui est $1 = (1, 0, 0, \cdots)$

Propriété 6 : $\deg(P \times Q) = $deq P+deg Q.

Théorème : $(\mathbb{K}[X], +, \times)$ est un anneau commutatif intègre, c'est à dire

$$\forall (P,Q) \in (\mathbb{K}[X])^2,\ P \times Q = 0 \Rightarrow P = 0 \text{ ou } Q = 0.$$

Remarque : $(\mathbb{K}[X], +, \times)$ n'est pas un corps.

1.4. Multiplication par un scalaire

Définition : On définit dans $\mathbb{K}[X]$ une loi externe $\cdot$ depuis le corps $\mathbb{K}$ par $\forall \lambda in \mathbb{K}, \forall P \in \mathbb{K}[X]$, où $P = (a_n)$ alors on définit $\lambda.P = (\lambda.a_n)$.

Théorème : $(\mathbb{K}[X], +, \cdot)$ est un espace vectoriel.

1.5. Générateur de $\mathbb{K}[X]$

Définition : On pose $X = (0, 1, 0, 0, \cdots)$. On remarque alors que $X^2 = (0, 0, 1, 0, . \cdots)$ et plus généralement, soit $n \in \mathbb{N}$, $X^n = (\underbrace{0, \cdots, 0}_{\text{n fois}}, 1, 0, 0, \cdots)$ avec $X^0 = 1$. Soit $P \in \mathbb{K}[X]$, tel que $P = (a_n)$ alors on peut réécrire $P = \sum_{k=0}^{\deg\ P} a_k X^k$.

Définition : X est appelé générateur de $\mathbb{K}[X]$, on l'appelle aussi indéterminée.

Définition : Soit $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble formé par les polynômes de degré inférieur ou égaux à n.

Théorème : $\forall n \in \mathbb{N},\ \mathbb{K}_n[X]$ est un $\mathbb{K}$-espace vectoriel.

Proposition : On identifie $\mathbb{K}_0[X]$ à $\mathbb{K}$ par la bijection $\varphi : \begin{array}{ccc} \mathbb{K}_0[X] & \to & \mathbb{K} \\ \lambda.1 & \mapsto & \lambda \end{array}$
D'où à présent on notera λ au lieu de $\lambda.1$.

1.6. Composition de polynômes

Définition : Soit $P(X) = \sum_{k=0}^{p} a_k.X^k$ et $Q(X) = \sum_{k=0}^{q} b_k.X^k$ alors on définit le polynôme $Q \circ P$ par $Q \circ P(X) = \sum_{i=0}^{q} b_i.\left(\sum_{k=0}^{p} a_k.X^k\right)^i$

2. Divisibilité

2.1. Définition

Définition : On dit que le polynôme P divise le polynôme Q si $\exists R \in \mathbb{K}[X]$ tel que $Q = P \times R$, ce qui se note $P|Q$. Si $P \neq 0$ alors R - s'il existe - est unique.

Proposition : Tout polynôme est divisble par tout polynôme de degré 0, et tout polynôme divise le polynôme nul.

Proposition : $|$ est une relation de préodre dans $\mathbb{K}[X]$. Soit $P \in \mathbb{K}[X]$, les éléments associés à P sont tous de la forme $\lambda.P$ avec $\lambda \neq 0$. Dans l'ensemble des polynômes unitaires, la relation $|$ devient une relation d'ordre.

2.2. Fonction polynômiale associée

Définition : Soit $P \in \mathbb{K}[X]$ définit par $P(X) = \sum_{k=0}^{p} a_k.X^k$ on associe l'application $\widetilde{P} : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & \sum_{k=0}^{p} a_k x^k \end{array}$

Théorème : Notons E l'ensemble des applications polynômiales, muni des lois $+$ et $\cdot$ E est un $\mathbb{K}$-espace vectoriel, et muni des lois $+$ et $\times$ est un anneau commutatif intègre. L'application $\varphi : \begin{array}{ccc} \mathbb{K}[X] & \to & E \\ P & \mapsto & \widetilde{P} \end{array}$ est un isomorphisme d'espace vectoriel et d'anneau si $\mathbb{K}$ est un corps infini tel $\mathbb{R}$ ou $\mathbb{C}$ et dans ce cas là il convient de confondre P et $\widetilde{P}$.

Propriété : Soit $P \in \mathbb{K}[X]$ de degré $\deg P \leq n$ admettant $m > n$ racines alors $P = 0$.

2.3. Divisibilité par $X - a$

Théorème : Soit $a \in \mathbb{K}$ et $P \in \mathbb{K}[X]$, $(X - a)|P \Leftrightarrow P(a) = 0$.

Corollaire : Soit $(a, b) \in \mathbb{K}^2$, et $P \in \mathbb{K}[X]$, alors

$$a \neq b,\ (X - a)|P \text{ et } (X - b)|P \Rightarrow (X - a)(X - b)|P.$$

Ce qui se généralise :

$$\forall P \in \mathbb{K}[X],\ \forall (a_1, \cdots, a_n) \in \mathbb{K}^n, \text{ si } \forall (i, j) \in \{1, \cdots, n\}^2, \text{ on a}$$
$$i \neq j \Rightarrow a_i \neq a_j \text{ et si } \forall i \in \{1, \cdots, n\} \text{ on a } (X - a_i)|P \text{ alors } \prod_{i=1}^{n}(X - a_i)\ |P.$$

2.4. Polynôme dérivé

Définition : Soit $P \in \mathbb{K}[X]$ tel que $P(X) = \sum_{k=0}^{p} a_k.X^k$. On appelle polynôme dérivé de P le polynôme noté P' définit par

$$P'(X) = \sum_{k=1}^{p} k a_k.X^{k-1} = \sum_{k=0}^{p-1}(k + 1)a_{k+1}.X^k.$$

Propriété 1 : $\forall (P, Q) \in (\mathbb{K}[X])^2,\ (P + Q)' = P' + Q'$.

Propriété 2 : $\forall \lambda \in \mathbb{K}, \forall P \in \mathbb{K}[X],\ (\lambda.P) = \lambda.P'$.

Propriété 3 : L'application $\varphi_D : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}[X] \\ P & \mapsto & P' \end{array}$ est un endormorphisme de $\mathbb{K}[X]$.

Propriété 4 : $\forall (P,Q) \in (\mathbb{K}[X])^2,\ (P \times Q)' = P' \times Q + P \times Q'$.

Définition : On défini par récurrence les dérivées successives d'un polynôme P par $\forall k \in \mathbb{N},\ P^{(k+1)} = \left(P^{(k)}\right)'$. Si $P(X) = \sum_{k=0}^{p} a_k X^k$ alors

$$\forall i \in \mathbb{N},\ P^{(i)}(X) = \sum_{k=i}^{p} \frac{k!}{(k-i)!} X^{k-i}.$$

Théorème : Formule de Liebniz : $\forall (P,Q) \in (\mathbb{K}[X])^2,\ \forall n \in \mathbb{N},\ (P \times Q)^{(n)} = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) P^{(k)} Q^{(n-k)}$

Théorème : Formule de Taylor : Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $p =$deg P, alors

$$P(X+a) = \sum_{k=0}^{p} \frac{P^{(k)}(a)}{k!}\ X^k$$

Remarque : Si on prend $a = 0$ alors on trouve $P(X) = \sum_{k=0}^{p} \frac{P^{(k)}(0)}{k!}\ X^k$ et donc on trouve $\forall n \in \mathbb{N},\ a_n = \frac{P^{(n)}(0)}{n!}$.

2.5. Divisibilité par $(X-a)^k$

Théorème : Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $k \in \mathbb{N}^*$.

$$(X-a)^k | P \ \Leftrightarrow\ P(a) = P'(a) = \cdots = P^{(k-1)}(a) = 0$$

Définition : On appelle racine du polynôme P tout élément α de $\mathbb{K}$ tel que $P(\alpha) = 0$, et on appelle multiplicité de α le plus petit entier k tel que $P^{(k)} \neq 0$, on note $k =$ mult α.
Si $\lambda =$ mult α alors par définition équivalente :

$$\forall i \in \{0, \cdots, \lambda - 1\},\ P^{(i)}(\alpha) = 0 \text{ et } P^{(\lambda)}(\alpha) \neq 0.$$

Théorème : Soit $P \in \mathbb{K}[X]$, et α une racine de P avec $\lambda =$ mult α. Alors $(X-\alpha)^\lambda | P$ et $(X-\alpha)^{\lambda+1} \nmid P$, ce qui nous donne $P(X) = (X-\alpha)^\lambda \times Q(X)$ avec $Q(\alpha) \neq 0$.

3. Division Euclidienne suivant les puissances croissantes

Théorème de la division Euclidienne :

$$\forall (A,B) \in (\mathbb{K}[X])^2 \ / \ B \neq 0, \ \exists !(Q,R) \in (\mathbb{K}[X])^2, \text{ tel que } \begin{cases} A = BQ + R \\ \deg R < \deg B \end{cases}$$

Remarque : Soit $A = \sum_{k=0}^{p} a_k X^k$ et $B = \sum_{k=0}^{q} b_k X^k$ avec $a_p \neq 0$, $b_q \neq 0$ et $p \geq q$. On effectue une division euclidienne selon les puissances croissantes donc on cherche à faire disparaitre $a_p X^p$ grâce à B. Et on obtient $A(X) = \frac{a_p}{b_q} X^{p-q} B(X) + A_1(X)$ et on recommence, on effectue la division euclidienne de $A_1(X) = A(X) - \frac{a_p}{b_q} X^{p-q} B(X)$ par $B(X)$ et on s'arrête quand le reste à un degré inférieur strictement à celui de B.

4. Factorisation

4.1. Polynôme irréductible

Définition : Soit $P \in \mathbb{K}[X]$ de degré $\deg P \geq 1$, on dit que P est irréductible si P n'admet pas de diviseur $Q \in \mathbb{K}[X]$ tel que $1 \leq \deg Q < \deg P$.

Remarque : Les polynômes de degré 1 sont irréductibles.

Définition : On dit qe $P \in \mathbb{K}[X]$ est scindé si P est un produit de polynôme du 1^{er} degré de $\mathbb{K}[X]$.

4.2. Factorisation dans $\mathbb{C}[X]$

Théorème de d'Alembert :

$$\forall P \in \mathbb{K}[X] \ / \ \deg P \geq 1, \ \exists \alpha \in \mathbb{C} \ / \ P(\alpha) = 0.$$

Corollaire : $\forall P \in \mathbb{K}[X]$ de degré $\deg P = n \geq 1$, et de terme dominant $a_n \neq 0$, alors $\exists (\alpha_1, \cdots, \alpha_n) \in \mathbb{C}^n$ tel que $P(X) = a_n . \prod_{k=1}^{n} (X - \alpha_k)$.

Théorème : Tous les polynômes sur $\mathbb{C}[X]$ et les seuls polynômes irréductibles sont ceux de degré 1.

4.2. Factorisation dans $\mathbb{R}[X]$

Théorème : Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 de la forme $P(X) = aX^2+bX+c$ avec $\Delta = b^2-4ac < 0$.

Corollaire : Tout polynôme de $\mathbb{R}[X]$ peut se factoriser dans $\mathbb{R}[X]$sous la forme d'un produit de polynômes de degré 1 et de degré 2 à discriminant $\Delta < 0$ donc sous la forme :

$$P(X) = \prod_{k=1}^{p}(a_kX + b_k)\prod_{j=1}^{q}(c_jX^2 + d_jX + e_j) \text{ avec } \forall k \in \{1, \cdots, p\}\ a_k \neq 0,$$
$$\forall j \in \{1, \cdots, q\}\ d_j^2 - 4c_je_j < 0 \text{ et } c_j \neq 0 \text{ et enfin } p + 2q = \deg P.$$

Mais tout polynôme de $\mathbb{R}[X]$ peut aussi se factoriser dans $\mathbb{C}[X]$ sous la forme de produit de polynômes de degré 1 dont les racines sont soit réelles soit conjuguées deux à deux, donc sous la forme :

$$P(X) = \prod_{k=1}^{p}(a_kX + b_k)\prod_{j=1}^{q}c_j(X - \alpha_j)(X - \overline{\alpha_i}) \text{ avec } \forall k \in \{1, \cdots, p\}\ a_k \neq 0,$$
$$\forall j \in \{1, \cdots, q\}\ c_j \neq 0 \text{ et } \alpha_i \in \mathbb{C} \setminus \mathbb{R} \text{ et enfin } p + 2q = \deg P.$$

5. Relation entre coefficients et racines

Théorème : Soit $P \in \mathbb{C}[X]$ de degré n et de racines $\alpha_1, \alpha_2, \cdots, \alpha_n$ distinctes ou confondues, on a donc $P(X) = a_n\prod_{i=1}^{n}(X - \alpha_i)$. $\forall k \in \{1, \cdots, n\}$, on pose $\sigma_k = \prod_{1\leqslant i_1<\cdots<i_k\leqslant n}\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_k}$ appelés polynômes symétriques élémentaire en les racines de P. Et on a alors la relation suivante :

$$\forall k \in \{1, \ldots, n\} \quad \sigma_k = (-1)^k\frac{a_{n-k}}{a_n}$$

6. Divisibilité dans l'anneau $\mathbb{K}[X]$

6.1. PGCD

Définition : Soit $P \in \mathbb{K}[X]$ on note l'ensemble des multiples de P de la façon suivante $(P) = \left\{P \times Q \ / \ Q \in \mathbb{K}[X]\right\}$. Soit $(P, Q) \in (\mathbb{K}[X])^2$ on définit la somme $(P) + (Q) = \left\{U \times P + V \times Q \ / \ (U, V) \in (\mathbb{K}[X])^2\right\}$

Proposition : $\forall P \in \mathbb{K}[X]$, (P) est un sous-groupe de $(\mathbb{K}[X], +)$.

Proposition : $\forall (P,Q) \in (\mathbb{K}[X])^2$, $(P)+(Q)$ est un sous-groupe de $(\mathbb{K}[X], +)$.

Proposition : $\forall (P,Q) \in (\mathbb{K}[X])^2$, $P|Q \Leftrightarrow (Q) \subset (P)$.

Proposition : $\forall (P,Q) \in (\mathbb{K}[X])^2$, $(P) = (Q) \Leftrightarrow P$ et Q sont associés $\Leftrightarrow \exists \lambda \in \mathbb{K} \ / \ P = \lambda.Q$.

Proposition : Soit $R \in (P)+(Q)$ alors $(R) \subset (P)+(Q)$.

Théorème : $\forall (P,Q) \in (\mathbb{K}[X])^2$, $\exists R \in \mathbb{K}[X]$ tel que $(P)+(Q) = (R)$.

Définition : Soit $(P,Q) \in (\mathbb{K}[X])^2$, On appelle $PGCD$ de P et Q, noté $P \wedge Q$ l'unique polyôme unitaire R tel que $(P)+(Q) = (R)$.

Théorème : Le $PGCD$ d'un couple (P,Q) est le polynôme unitaire accocié au dernier reste non nul dans l'algorithme d'Euclide. Algorithme composé de divisions euclidiennes successives de la même manière que dans $\mathbb{Z}$.

6.2. PPCM

Proposition : Soit $(P,Q) \in (\mathbb{K}[X])^2$ non nuls, $\exists M \in \mathbb{K}[X] \ / \ (M) = (P) \cap (Q)$.

Définition : On appelle $PPCM$ d'un couple $(P,Q) \in (\mathbb{K}[X])^2$ non nuls - noté $P \vee Q$ - l'unique polynôme unitaire $M \in \mathbb{K}[X]$ tel que $(M) = (P) \cap (Q)$.

6.3. Polynôme premiers entre eux

Définition : On dit que les polynômes P et Q sont premiers entre eux si $P \wedge Q = 1$.

Théorème de Bézout :
$\forall (P,Q) \in (\mathbb{K}[X])^2 \ / \ P \wedge Q = 1, \ \exists (U,V) \in (\mathbb{K}[X])^2 \ / \ UP + VQ = 1$.

Théorème de Gauss :
$\forall (P,Q,R) \in (\mathbb{K}[X])^3, \ P|QR$ et $P \wedge Q = 1 \Rightarrow P|Q$.

Corollaire : $P|R$, $Q|R$ et $P \wedge Q = 1 \ \Rightarrow PQ|R$.

7. Décomposition en élément simple d'une fraction rationnelle

7.1. Corps $\mathbb{K}(X)$

Définition : On définit l'ensemble des fractions rationnelles noté $\mathbb{K}(X)$ par $\mathbb{K}(X) = \left\{ F(X) = \dfrac{P(X)}{Q(X)} \ / \ (P,Q) \in \mathbb{K}[X] \times \mathbb{K}[X]^* \right\}$.

On peut voir que $\dfrac{P}{Q} = \dfrac{R}{S} \Leftrightarrow PS = QR$ dans $\mathbb{K}[X]$

On définit une loi + par : $\dfrac{P}{Q} + \dfrac{R}{S} = \dfrac{PS+QR}{QS}$ d'élément neutre 0 comme dans $\mathbb{K}[X]$, $-\left(\dfrac{P}{Q}\right) = \dfrac{-P}{Q} = \dfrac{P}{-Q}$. On remarque que $\forall P \in \mathbb{K}[X]^*,\ \dfrac{0}{P} = 0$.

On définit une loi $\times$ par : $\dfrac{P}{Q} \times \dfrac{R}{S} = \dfrac{PR}{QS}$ d'élément neutre 1 comme dans $\mathbb{K}[X]$. Soit $\dfrac{P}{Q}$ avec $P \neq 0$, alors on a $\left(\dfrac{P}{Q}\right)^{-1} = \dfrac{Q}{P}$ alors on remarque $\forall P \in \mathbb{K}[X]^*,\ \dfrac{P}{P} = 1$.

Définition : On appelle forme irréductible de $F \in \mathbb{K}(X)$ l'unique écriture de F sous la forme $\dfrac{P}{Q}$ où Q est unitaires et $P \wedge Q = 1$.

Définition : Soit $F = \dfrac{P}{Q}$ écrite sous forme irréductible, on appelle pôle de F toute racine de Q. On appelle multiplicité du pôle α de F la multiplicité de α dans Q.

7.2. Fonctions rationnelles associées à une fraction rationnelle.

Définition : A une fraction rationnelle $F = \dfrac{P}{Q}$ on peut associer la fonction rationnelle $\widetilde{F} : \begin{array}{ccc} D & \to & \mathbb{K} \\ x & \mapsto & \dfrac{P(x)}{Q(x)} \end{array}$ où $D = \mathbb{K} \setminus \left\{ \alpha \in \mathbb{K} \ / \ Q(\alpha) = 0 \right\}$.

Remarque : $\widetilde{F}$ dépend du représentant $\dfrac{P}{Q}$ choisit, si $\dfrac{P}{Q}$ est la forme irréductible de F alors D sera le plus grand ensemble possible sur lequel $\widetilde{F}$ sera définie,

on le note ici D_{max}, mais si $P \wedge Q = R \neq 1$ donc de degré deg $R \geqslant 1$ on peut alors écrire $F = \dfrac{RP'}{RQ'}$ où $\dfrac{P'}{Q'}$ est la forme irreductible de F, alors ici $D = D_{max} \setminus \left\{\alpha \in \mathbb{K} \ / \ R(\alpha) = 0\right\}$, donc $\widetilde{F}$ ne sera pas défini en les racines de R si distinctes de celles de Q'. En tout point où deux formes de $\widetilde{F}$ sont définies, elles sont égales.

7.3. Décomposition en élément simple

Définition : On appelle élément simple dans $\mathbb{C}(X)$ toute fraction rationnelle de la forme $\dfrac{a}{(X-\alpha)^n}$ où $a \in \mathbb{C}, \alpha \in \mathbb{C}$ et $n \in \mathbb{N}^*$.

Lemme : Toute fraction $F = \dfrac{P}{Q}$ sous forme irréductible, se décompose de manière unique sous la forme $F = E + \dfrac{R}{Q}$ avec deg $R <$ deg Q.

Théorème : Soit $F = \dfrac{P}{Q} \in \mathbb{C}(X)$ mise sous forme irréductible, de pôles $\alpha_1, \cdots, \alpha_n$ de multiplicités respectives $\beta_1, \cdots, \beta_n$. Soit $P = EQ + R$ la division euclidienne de P par Q. Alors F peut se décomposer en éléments simples sous la forme unique :

$$\begin{aligned} F(X) = E(X) &+ \frac{A_{\beta_1,\alpha_1}}{(X-\alpha_1)^{\beta_1}} + \frac{A_{\beta_1-1,\alpha_1}}{(X-\alpha_1)^{\beta_1-1}} + \cdots + \frac{A_{1,\alpha_1}}{(X-\alpha_1)} \\ &+ \frac{A_{\beta_2,\alpha_2}}{(X-\alpha_2)^{\beta_2}} + \frac{A_{\beta_2-1,\alpha_2}}{(X-\alpha_2)^{\beta_2-1}} + \cdots + \frac{A_{1,\alpha_2}}{(X-\alpha_2)} \\ &+ \cdots \\ &+ \frac{A_{\beta_n,\alpha_n}}{(X-\alpha_n)^{\beta_n}} + \frac{A_{\beta_n-1,\alpha_n}}{(X-\alpha_n)^{\beta_n-1}} + \cdots + \frac{A_{1,\alpha_n}}{(X-\alpha_n)} \end{aligned}$$

où $A_{\beta_1,\alpha_1}, ..., A_{\beta_{n-1},\alpha_{n-1}}$ et A_{β_n,α_n} sont tous non nuls.

Définition : $E(X)$ s'appelle partie entière de la fraction rationnelle $F(X)$, et $\dfrac{A_{\beta_j,\alpha_j}}{(X-\alpha_j)^{\beta_j}} + \dfrac{A_{\beta_j-1,\alpha_j}}{(X-\alpha_j)^{\beta_j-1}} + \cdots + \dfrac{A_{1,\alpha_j}}{(X-\alpha_j)}$ est appelée la forme polaire de F relativement au pôle α_j.

Remarque : Si deg $P <$ deg Q alors $E(X) = 0$.

Proposition : Soit $F(X) = \dfrac{P(X)}{Q(X)}$ sous forme irréductible de pôles $\alpha_1, \cdots, \alpha_n$ de multiplicités respectives $\beta_1, \cdots, \beta_n$.
$Q(X) = \prod_{i=1}^{n}(X-\alpha_i)^{\beta_i}$. On note $Q_j(X) = \prod_{i\neq j}^{n}(X-\alpha_i)^{\beta_i} = \dfrac{Q(X)}{(X-\alpha_j)^{\beta_j}}$.
Alors on trouve les premiers coefficients $A_{\beta_j,\alpha_j} = \dfrac{P(\alpha_j)}{Q_j(\alpha_j)}$.

Pour les autres coefficients :

1) on peut remplacer X par x_0 qui n'est pas un pôle de F et obtenir un sytème :

$$\begin{aligned}\frac{P(x_0)}{Q(x_0)} = E(x_0) &+ \frac{A_{\beta_1,\alpha_1}}{(x_0-\alpha_1)^{\beta_1}} + \frac{A_{\beta_1-1,\alpha_1}}{(x_0-\alpha_1)^{\beta_1-1}} + \cdots + \frac{A_{1,\alpha_1}}{(x_0-\alpha_1)} \\ &+ \frac{A_{\beta_2,\alpha_2}}{(x_0-\alpha_2)^{\beta_2}} + \frac{A_{\beta_2-1,\alpha_2}}{(x_0-\alpha_2)^{\beta_2-1}} + \cdots + \frac{A_{1,\alpha_2}}{(x_0-\alpha_2)} \\ &+ \cdots \\ &+ \frac{A_{\beta_n,\alpha_n}}{(x_0-\alpha_n)^{\beta_n}} + \frac{A_{\beta_n-1,\alpha_n}}{(x_0-\alpha_n)^{\beta_n-1}} + \cdots + \frac{A_{1,\alpha_n}}{(x_0-\alpha_n)}\end{aligned}$$

2) on a $\dfrac{P}{Q} = E + \dfrac{R}{Q}$ et alors on multiplie par X, on obtient donc

$$\begin{aligned}\frac{XR(X)}{Q(X)} = &\frac{A_{\beta_1,\alpha_1}X}{(X-\alpha_1)^{\beta_1}} + \frac{A_{\beta_1-1,\alpha_1}X}{(X-\alpha_1)^{\beta_1-1}} + \cdots + \frac{A_{1,\alpha_1}X}{(X-\alpha_1)} \\ &+ \frac{A_{\beta_2,\alpha_2}X}{(X-\alpha_2)^{\beta_2}} + \frac{A_{\beta_2-1,\alpha_2}X}{(X-\alpha_2)^{\beta_2-1}} + \cdots + \frac{A_{1,\alpha_2}}{(X-\alpha_2)} \\ &+ \cdots \\ &+ \frac{A_{\beta_n,\alpha_n}X}{(X-\alpha_n)^{\beta_n}} + \frac{A_{\beta_n-1,\alpha_n}X}{(X-\alpha_n)^{\beta_n-1}} + \cdots + \frac{A_{1,\alpha_n}X}{(X-\alpha_n)}\end{aligned}$$

et on fait tendre X vers $+\infty$, on obtient :

$$\lim_{X\to+\infty} \frac{XR(X)}{Q(X)} = A_{1,\alpha_1} + A_{1,\alpha_2} + \cdots + A_{1,\alpha_n}.$$

c) si $F \in \mathbb{R}(X)$, les coefficients de même ordre des racines conjuguées sont conjugués. C'est à dire $A_{j,\alpha} = \overline{A_{j,\overline{\alpha}}}$

d) utiliser la partité possible de F pour déduire d'éventuels rapports entre les coefficients, ou l'annulation de certains.

Théorème : Soit $P(X) = K.\prod_{i=1}^{n}(X-\alpha_i)^{\beta_i}$ avec $K \in \mathbb{C}^*$. Alors on a la décomposition en éléments simples suivante $\dfrac{P'(X)}{P(X)} = \sum_{i=1}^{n} \dfrac{\beta_i}{X-\alpha_i}$.

Proposition : La décomposition en éléments simples permet de calculer des primitives de toute fraction rationnelle, il suffit pour cela de savoir :

$\forall a \in \mathbb{C},\ \alpha \in \mathbb{N}$ avec $\alpha \geqslant 2$ alors on a :

$$\int \frac{1}{(t-a)^{\alpha}}\ dt = \frac{1}{1-\alpha} \cdot \frac{1}{(t-a)^{\alpha-1}} + c \ \text{ où } c \in \mathbb{C}.$$

Si $\mathcal{I}_m(a) \neq 0$ alors :

$$\int \frac{1}{(t-a)}\ dt = \ln|t-a| + i.\text{Arctan}\left(\frac{t-\mathcal{R}_e(a)}{\mathcal{I}_m(a)}\right)$$

Si $\mathcal{I}_m(a) = 0 \Leftrightarrow a \in \mathbb{R}$ alors :

$$\int \frac{1}{(t-a)}\ dt = \ln|t-a|$$

CHAPITRE V : Espaces vectoriels de dimension finie

1. Familles génératrices, libres et bases

1.1. Combinaison linéaire de vecteurs

Définition : On appelle combinaison linéaire des p vecteurs $u_1, \cdots, u_p$ du K-espace vectoriel E tout vecteur v s'écrivant $v = \sum_{i=1}^{p} \lambda_i.u_i$ où $\forall i,\ \lambda_i \in K$

Proposition : Tout espace vectoriel est stable par combinaison linéaire.

Proposition : Soit $f \in \mathcal{L}(E,F)$, $(u_1, \cdots, u_p) \in E^n$, $(\lambda_1, \cdots, \lambda_p) \in K^p$, alors

$$f\left(\sum_{i=1}^{p} \lambda_i.u_i\right) = \sum_{i=1}^{p} \lambda_i.f(u_i)$$

Définition : On appelle sous-espace vectoriel engendré par la famille de vecteurs $(u_1, \cdots, u_p) \in E^p$ l'ensemble des combinaisons linéaires des p-vecteurs $(u_1, \cdots, u_p)$. On le note $Vect(u_1, \cdots, u_p)$.

Proposition : $Vect(u_1, \cdots, u_p)$ est un sous-espace vectoriel de E.

Remarque : $Vect(u_1, \cdots, u_p)$ est le sous-espace vectoriel egendré par la partie $A = \{u_1, \cdots, u_p\}$ précédemment noté $Vect(A)$ est aussi égal à l'intersection des sous-espaces vectoriels contenant A.

1.2. Famille génératrice

Définition : Soit F un sous-espace vectoriel de E. On dit que la famille $(u_1, \cdots, u_p) \in E^p$ est génératrice de F si tout vecteur de F est une combinaison linéaire des p-vecteurs $u_1, \cdots, u_p$ donc si $Vect(u_1, \cdots, u_p) = F$.

Remarque : Soit $(u_1, \cdots, u_p)$ une famille génératrice de F et soit les vecteurs $(u_{p+1}, \cdots, u_{p+n}) \in E^n$, alors $(u_1, \cdots, u_p, u_{p+1}, \cdots, u_{p+n})$ est une famille génératrice de F.

Proposition : Soit $(u_1, \cdots, u_p) \in E^p$ une famille génératrice du sous-espace vectoriel F ; pour que la famille $(v_1, \cdots, v_n) \in F^n$ soit génératrice de F il faut et il suffit que tout u_i soit combinaison linéaire de la famille $(v_1, \cdots, v_n)$.

1.3 Familles libres, familles liées

Définition : Soit $(u_1, \cdots, u_p)$ une famille de p-vecteurs du K-espace vectoriel E, on dit que la famille $(u_1, \cdots, u_p)$ est libre si :

$$\forall(\lambda_1, \cdots, \lambda_p) \in K^p,\ \sum_{i=1}^{p} \lambda_i u_i = \overrightarrow{0} \Rightarrow \forall i \in \{1, \cdots, p\},\ \lambda_i = 0.$$

Dans ce cas on dit que les vecteurs sont linéairement indépendants.

On dit qu'une famille $(u_1, \cdots, u_p)$ est liée si elle n'est pas libre.

Proposition : $(u_1, \cdots, u_p)$ est liée $\Leftrightarrow \exists(\lambda_1, \cdots, \lambda_p) \in \mathbb{K}^p \setminus \{(0, \cdots, 0)\}$ tel que $\sum_{i=1}^{p} \lambda_i u_i = \overrightarrow{0}$.

Remarques : 1) Si la famille $(u_1, \cdots, u_p)$ est liée alors toute famille $(u_1, \cdots, u_p, u_{p+1}, \cdots, u_{p+n})$ est liée.

2) Toute sous-famille d'une famille libre est libre.

3) Toute famille contenant le vecteur $\overrightarrow{0}$ est liée.

Proposition : Pour qu'une famille soit liée il faut et il suffit qu'un vecteur soit combinaison linéaire des autres vecteurs de la famille.

Théorème : Soit $n \in \mathbb{N}^*$, soit $(u_1, \cdots, u_n)$ une famille de n vecteurs et $(v_1, \cdots, v_{n+1})$ une famille de $n+1$ vecteurs combinaison linéaire de la famille $(u_1, \cdots, u_n)$, alors $(v_1, \cdots, v_{n+1})$ est liée.

1.4. Base

Définition : On dit que la famille $(u_1, \cdots, u_n)$ est une base du sous-espace vectoriel F du K-espace vectoriel E si elle est libre et génératrice de F.

1.5. Coordonnées

Théorème : Soit $\mathcal{B} = (u_1, \cdots, u_n)$ une base du sous-espace vectoriel F du K-espace vectoriel E, alors pour tout vecteur $v \in F$ il existe un unique n-uplet $(x_1, \cdots, x_n) \in K^n$ tel que $v = \sum_{i=1}^{n} x_i u_i$.

Définition : La famille $(x_1, \cdots, x_n)$ est appelée famille de coordonnées du vecteur v dans la base $\mathcal{B} = (u_1, \cdots, u_n)$.
x_i est appelée $i^{ème}$ coordonnée du vecteur v dans la base $\mathcal{B}$.

2. Dimension

2.1. Théorème de la base incomplète

Définition : On dit que le K-espace vectoriel E est de dimension finie si E admet une famille génératrice finie.

Théorème de la base incomplète :
Soit E un espace vectoriel de dimension finie et non réduit à $\left\{\overrightarrow{0}\right\}$. Soit $(u_1, \cdot, u_m)$ une famille libre de E alors on peut compléter cette famille en $(u_1, \cdots, u_m, \cdots, u_n)$ telle que elle soit une base de E.

Remarque : 1) Ce théorème prouve l'éxistence d'une base pour un K-espace vectoriel de dimension finie, pour ce il suffit de compléter une famille trivialement libre (u) avec $u \neq \overrightarrow{0}$.

2) En pratique on complète une famille libre avec des vecteurs d'une base connue.

2.2. Dimension d'un espace vectoriel

Théorème : Soient les 3 familles suivantes :

$\mathcal{U} = (u_1, \cdots, u_p)$ libre,
$(e_1, \cdots, e_n)$ base de E,
$\mathcal{V} = (v_1, \cdots, v_q)$ génératrice de E.

Alors $p \leqslant n \leqslant q$. De plus si :

1) $p = n$ alors $\mathcal{U}$ est une base de E
2) $q = n$ alors $\mathcal{V}$ est une base de E.

Remarque : Toutes les bases d'un espace vectoriel E ont donc même nombre de vecteurs si celui-ci n'est pas réduit à $\left\{\overrightarrow{0}\right\}$.

Définition : On appelle dimension d'un espace vectoriel E le nombre de vecteurs dans une base de E. On la note dim E, en précisant parfois sur quel corps E est défini on note $\dim_K E$.
Par convention dim $\left\{\overrightarrow{0}\right\} = 0$.

Proposition : Soit E un espace vectoriel de dimension n, alors toute famille libre ou génératrice de E de n vecteurs est une base de E.

2.3. Dimension d'un sous-espace vectoriel

Définition : On appelle dimension du sous-espace vectoriel F de E la dimension de l'espace vectoriel F.

Proposition : Tout sous-espace vectoriel F d'un espace vectoriel E de dimension finie est de dimension finie et dim $F \leqslant$ dim E.

Théorème : Soient F et G deux sous-espaces vectoriels de E de dimension finie alors :

$$\dim(F+G) + \dim(F \cap G) = \dim F + \dim G.$$

Remarque : si F et G sont en somme directe alors dim$(F \oplus G)$ =dim F + dim G.

Remarque : si F est un sous-espace vectoriel de E de dimension finie et si dim F =dim E alors $F = E$.

2.4. Existence de supplémentaire

Proposition : Tout sous-espace vectoriel F d'un espace vectoriel E de dimension finie admet un sous-espace vectoriel G de E qui lui est supplémentaire.

2.5. Rang d'une famille de vecteurs

Définition : On appelle rang de la famille $U = (u_1, \cdots, u_n)$ de vecteurs de E la dimension du sous-espace vectoriel $Vect(U)$. Si U est libre alors c'est une base de $Vect(U)$ et donc dim $Vect(U) = n$. Si U est liée alors $\exists u_0$ un des vecteurs de U qui est combinaison linéaire des autres et dim $Vect(U) < n$.

2.6. Dimension d'un espace vectoriel produit

Proposition : Soit E et F deux K-espaces vectoriels de dimension finie alors :

$$\dim E \times F = \dim E + \dim F.$$

CHAPITRE VI : Applications linéaires et matrices

1. Application linéaires

1.1. Rappels

Rappels : Soient E et F deux K-espaces vectoriels de dimension finie, $\mathcal{L}(E,F)$ est l'ensemble des applications linéaires de E dans F. $\mathcal{L}(E)$ l'ensemble des endomorphismes de E. Soit $f \in \mathcal{L}(E,F)$, alors on appelle noyaux de f l'ensemble $\ker f = \left\{x \in E \ / \ f(x) = 0\right\}$ et l'image de f l'ensemble $\text{Im } f = f(E)$.

1.2. Théorème fondamental

Théorème : Une application linéaire est totalement déterminée par l'image d'une base. C'est à dire, étant la famille $\mathcal{B} = (e_1, \cdots, e_n)$ base de E et une famille de vecteurs $(u_1, \cdots, u_n)$ de F. Alors il existe une unique application linéaire de E dans F telle que $\forall i \in \{1, \cdots, n\}$ $f(e_i) = u_i$.

Remarque : Etant donnée une famille de vecteurs $(u_1, \cdots, u_n)$ de E alors il existe une unique application linéaire φ de K^n dans E liée à la base canonique $(e_1, \cdots, e_n)$ de K^n définie par

$$\begin{array}{ccc} K^n & \to & E \\ v = \displaystyle\sum_{i=1}^{n} x_i e_i & \mapsto & \displaystyle\sum_{i=1}^{n} x_i u_i \end{array}$$

Si $(u_1, \cdots, u_n)$ est libre alors φ est injective.
Si $(u_1, \cdots, u_n)$ est génératrice alors φ est surjective.
Si $(u_1, \cdots, u_n)$ est une base alors φ est un isomorphisme.

1.3. Isomorphisme

Théorème : Soit $f \in \mathcal{L}(E,F)$ avec $n = \dim E$ et $p = \dim F$.

f est un isomorphisme $\Leftrightarrow n = p$ et f injective.
$\Leftrightarrow$ l'image d'une base de E est une base de F.

Lemme 1 : Soit $(u_1, \cdots, u_n)$ une famille libre de E et $f \in \mathcal{L}(E,F)$ injective, alors $(f(u_i, \cdots, f(u_n))$ est une famille libre de F.

Lemme 2 : Soit $(u_1, \cdots, u_n)$ une famille génératrice de E et $f \in \mathcal{L}(E, F)$ alors $(f(u_1), \cdots, f(u_n))$ est génératrice de Im f.

Remarque : Deux K-espaces vectoriels de même dimension finie sont isomorphes, et tout K-espace vectoriel de dimension n est isomorphe à K^n.

1.4. Théorème de la dimension

Proposition : Soit $f \in \mathcal{L}(E, F)$, et G un sous-espace vectoriel de E supplémentaire à ker f. Alors $f_{|G}$ est un isomorphisme de G sur Im f.

Théorème de la dimension :

$$\text{Soit } f \in \mathcal{L}(E, F) \text{ alors } \dim E = \dim \ker f + \dim \text{Im } f.$$

Corollaire : Soit $f \in \mathcal{L}(E, F)$ avec dim E = dim F alors :

$$f \text{ injective} \Leftrightarrow f \text{ surjective} \Leftrightarrow f \text{ bijective.}$$

1.5. Rang d'une application linéaire

Définition : Soit $f \in \mathcal{L}(E, F)$ alors on appelle rang de f noté et défini par :

$$\text{rg } f = \text{Im } f$$

Proposition : Soient $(e_1, \cdots, e_n)$ une base de E et $f \in \mathcal{L}(E, F)$ alors le rang de f est égal au rang de la famille $(f(e_1), \cdots, f(e_n))$.

1.6. Hyperplan

Définition : On appelle hyperplan d'un K-espace vectoriel E tout sous-espace de E admettant un sous-espace vectoriel de E supplémentaire de dimension 1.

Remarque : Si E est de dimension finie n, les hyperplans de E sont les sous-espaces vectoriel de E de dimension $n - 1$.

Rappel : On appelle forme linéaire de E un K espace vectoriel, toute application linéaire de E dans K.

Théorème : Soit E un espace vectoriel de dimension finie, le noyau d'une

forme linéaire non nulle surl E est un hyperplan et réciproquement tout hyperplan de E est le noyau d'une forme linéaire non nulle sur E.

Définition : Soit f une forme linéaire non nulle sur E de dimension finie de noyau l'hyperplan H. On dit alors que $f(u) = 0$ ($\Leftrightarrow u \in H$) est une équation cartésienne de H.

2. Matrices

2.1. Matrice d'une application linéaire

Remarque : D'après le théorème fondamental tout morphisme $f \in \mathcal{L}(E, F)$ est totalement déterminée par l'image d'une base $\mathcal{B} = (e_1, \cdots, e_q)$ de E.
On note $f(\mathcal{B}) = (f(e_1), \cdots, f(e_q))$, et on note relativement à une base $\mathcal{B}' = (f_1, \cdots, f_p)$ de F la $i^{ème}$ coordonnée de $f(e_j)$ sous la forme $a_{i,j}$.
Ce qui nous donne :

$$\begin{cases} f(e_1) = a_{1,1}f_1 + a_{2,1}f_2 + \cdots + a_{p,1}f_p \\ \vdots \\ f(e_i) = a_{1,i}f_1 + a_{2,i}f_2 + \cdots + a_{p,i}f_p \\ \vdots \\ f(e_q) = a_{1,q}f_1 + a_{2,q}f_2 + \cdots + a_{p,q}f_p \end{cases}$$

Donc f est totalement déterminée par le tableau de coordonnées suivant :

$$\begin{array}{cccc} \left(\begin{array}{cccc} a_{1,1} & a_{1,2} & \cdots & a_{1,q} \\ a_{2,1} & a_{2,2} & & a_{2,q} \\ \vdots & & \ddots & \vdots \\ a_{p,1} & a_{p,2} & \cdots & a_{p,q} \end{array}\right) & \begin{array}{c} \leftarrow f_1 \\ \leftarrow f_2 \\ \vdots \\ \leftarrow f_p \end{array} \\ \begin{array}{cccc} \uparrow & \uparrow & & \uparrow \\ f(e_1) & f(e_2) & \cdots & f(e_q) \end{array} & \end{array}$$

Définition : Ce tableau est appelé matrice de f relativement aux bases $\mathcal{B} = (e_1, \cdots, e_q)$ et $\mathcal{B}' = (f_1, \cdots, f_p)$ que l'on note :

$$M_{\mathcal{B},\mathcal{B}'}f = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,q} \\ a_{2,1} & a_{2,2} & & a_{2,q} \\ \vdots & & \ddots & \vdots \\ a_{p,1} & a_{p,2} & \cdots & a_{p,q} \end{pmatrix}$$

2.2. Matrice de type (p, q)

Définition : Une matrice (p, q) est un tableau formé de coefficients $a_{i,j} \in \mathbb{K}$ composée de p lignes et q colonnes.
La matrice A formée des coefficients $a_{i,j}$ peut s'écrire sous forme réduite :

$$A = (a_{i,j})_{p,q}.$$

On note $\mathcal{M}_{p,q}(\mathbb{K})$ l'ensemble formé par les matrices de type (p, q) à coefficients dans $\mathbb{K}$.
On notera $\mathcal{M}_n(\mathbb{K})$ l'ensemble des matrices carrées à n lignes et n colonnes au lieu de $\mathcal{M}_{n,n}(\mathbb{K})$.

Proposition : Soient $A = (a_{i,j})_{p,q}$ et $B = (b_{i,j})_{p,q}$ de $\mathcal{M}_{p,q}(\mathbb{K})$. Alors :

$$A = B \Leftrightarrow \forall (i, j) \in \{1, \cdots, p\} \times \{1, \cdots, q\} \text{ on a } a_{i,j} = b_{i,j}$$

Définition : On définit sur $\mathcal{M}_{p,q}(\mathbb{K})$ une addition par :

$\forall (A, B) \in (\mathcal{M}_{p,q}(\mathbb{K}))^2$ avec $A = (a_{i,j})_{p,q}$ et $B = (b_{i,j})_{p,q}$ on donne :

$$A + B = (c_{i,j})_{p,q} \text{ avec } c_{i,j} = a_{i,j} + b_{i,j}.$$

Théorème : $(\mathcal{M}_{p,q}(\mathbb{K}), +)$ est un groupe commutatif.

Définition : On définit sur $\mathcal{M}_{p,q}(\mathbb{K})$ une multiplication externe $\cdot$ par :

$\forall \lambda \in \mathbb{K},\ \forall A \in \mathcal{M}_{p,q}(\mathbb{K})$ avec $A = (a_{i,j})_{p,q}$ on donne :

$$\lambda.A = (b_{i,j})_{p,q} \text{ avec } b_{i,j} = \lambda a_{i,j}.$$

Théorème : $(\mathcal{M}_{p,q}(\mathbb{K}), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel de dimension pq donc isomorphe à $\mathbb{K}^{pq}$.

Définition :
Les matrices de $\mathcal{M}_{n,1}(\mathbb{K})$ sont appelées matrices colonnes d'ordre n.
Les matrices de $\mathcal{M}_{1,n}(\mathbb{K})$ sont appelées matrices lignes d'ordre n.
Les matrices de $\mathcal{M}_n(\mathbb{K})$ sont appelées matrices carrées d'ordre n.

2.3. Matrice représentative d'une application linéaire relativement à des bases données

Définition : On appelle matrice de l'application linéaire $f \in \mathcal{L}(E,F)$ relativement aux bases $\mathcal{B} = (e_1, \cdots, e_q)$ de E et $\mathcal{B}' = (f_1, \cdots, f_p)$ une base de F.
Soit la matrice $M_{\mathcal{B},\mathcal{B}'} f = (a_{i,j})_{p,q}$ où $f(e_j) = \sum_{i=1}^{p} a_{i,j} f_i$.

$$M_{\mathcal{B},\mathcal{B}'} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,q} \\ a_{2,1} & a_{2,2} & & a_{2,q} \\ \vdots & & \ddots & \vdots \\ a_{p,1} & a_{p,2} & \cdots & a_{p,q} \\ \uparrow & \uparrow & & \uparrow \\ f(e_1) & f(e_2) & \cdots & f(e_q) \end{pmatrix} \begin{matrix} \\ \leftarrow f_1 \\ \leftarrow f_2 \\ \vdots \\ \leftarrow f_p \\ \\ \end{matrix}$$

Si $f \in \mathcal{L}(E)$ avec $\mathcal{B}$ une base de E alors on note $M_{\mathcal{B}} f = M_{\mathcal{B},\mathcal{B}} f$.

Théorème d'isomorphisme : Soit $\mathcal{B}$ une base de E et $\mathcal{B}'$ une base de F où E et F sont deux $\mathbb{K}$-espaces vectoriels. L'application $\varphi : \begin{matrix} \mathcal{L}(E,F) & \to & \mathcal{M}_{p,q}(\mathbb{K}) \\ f & \mapsto & M_{\mathcal{B},\mathcal{B}'} f \end{matrix}$ est un isomorphisme de $\mathbb{K}$-espace vectoriel.

Corollaire : Si $\dim E = q$ et $\dim F = p$ alors :

$$\dim \mathcal{L}(E,F) = \dim \mathcal{M}_{p,q}(\mathbb{K}) = pq.$$

Remarque : L'isomorphisme φ n'est pas canonique mais dépend clairement des bases $\mathcal{B}$ et $\mathcal{B}'$. Or il existe un isomorphisme canonique entre $\mathcal{L}(\mathbb{K}^q, \mathbb{K}^p)$ et $\mathcal{M}_{p,q}(\mathbb{K})$ qui est $\psi : \begin{matrix} \mathcal{L}(\mathbb{K}^q, \mathbb{K}^p) & \to & \mathcal{M}_{p,q}(\mathbb{K}) \\ f & \mapsto & M_{\mathcal{B}_q,\mathcal{B}_p} f \end{matrix}$ où $\forall n \in \mathbb{N}^*$, $\mathcal{B}_n$ est la base canonique de $\mathbb{K}^n$.

2.4. Multiplication de matrices

Proposition : Soit $f \in \mathcal{L}(E,F)$ et $g \in \mathcal{L}(F,G)$ où E, F et G sont trois $\mathbb{K}$-espaces vectoriels de dimension finie. Soit $\mathcal{B} = (e_1, \cdots, e_r)$ une base de E, $\mathcal{B}' = (f_1, \cdots, f_q)$ une base de F et $\mathcal{B}'' = (g_1, \cdots, g_p)$ une base de G.
Soit $A = M_{\mathcal{B},\mathcal{B}'} f = (a_{i,j})_{q,r}$ et $B = M_{\mathcal{B}',\mathcal{B}''} g = (b_{i,j})_{p,q}$.

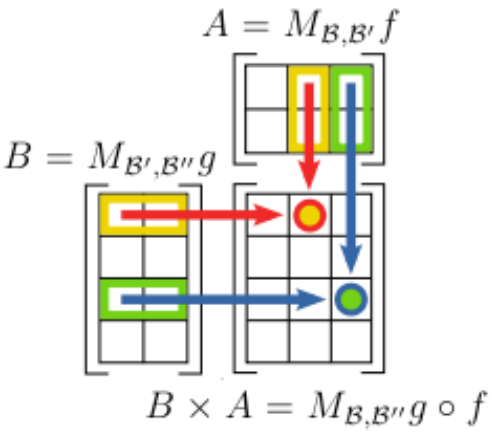
On a $f(e_j) = \sum_{i=1}^{q} a_{i,j} f_i$ et $g(f_i) = \sum_{k=1}^{p} b_{k,i} g_k$.

Ce qui nous donne :

$$g \circ f(e_j) = \sum_{k=1}^{p} \left(\sum_{i=1}^{q} b_{k,i} a_{i,j} \right) g_k.$$

On pose $c_{i,j} = \sum_{k=1}^{q} b_{i,k} a_{k,j}$ et on obtient $g \circ f(e_j) = \sum_{i=1}^{p} c_{i,j} g_i$. Donc la matrice de $g \circ f$ est $M_{\mathcal{B},\mathcal{B}''} g \circ f = (c_{i,j})_{p,r} = \left(\sum_{k=1}^{q} b_{i,k} a_{k,j} \right)_{p,r}$

Définition : Soit $A = (a_{i,j})_{q,r}$ et $B = (b_{i,j})_{p,q}$, alors on définit $B \times A$ par $B \times A = (c_{i,j})_{p,r}$ avec $c_{i,j} = \sum_{k=1}^{q} b_{i,k} a_{k,j}$. Si $A = M_{\mathcal{B},\mathcal{B}'} f$ et $B = M_{\mathcal{B}',\mathcal{B}''} g$ alors $B \times A = M_{\mathcal{B},\mathcal{B}''} g \circ f$. En pratique on multiplie les lignes de B avec les colonnes de A comme le montre le schéma suivant :



Remarque : Dans un produit $B \times A$ le nombre de colonnes de B doit être égal au nombre de lignes de A ce qui se voit sur le dessin précédent.

Propriété 1 : $M_{\mathcal{B}',\mathcal{B}''} g \times M_{\mathcal{B},\mathcal{B}'} f = M_{\mathcal{B},\mathcal{B}''} g \circ f$.

Propriété 2 : $\times$ est associative

$$\forall (A,B,C) \in \mathcal{M}_{p,q}(\mathbb{K}) \times \mathcal{M}_{q,r}(\mathbb{K}) \times \mathcal{M}_{r,s}(\mathbb{K}) \text{ on a :}$$
$$A \times (B \times C) = (A \times B) \times C$$

Propriété 3 : $\times$ est distributive :

$$\begin{cases} \forall A \in \mathcal{M}_{p,q}(\mathbb{K}) \text{ et } \forall (B,C) \in (\mathcal{M}_{q,r}(\mathbb{K}))^2 \ A \times (B+C) = A \times B + A \times C \\ \forall (A,B) \in (\mathcal{M}_{p,q}(\mathbb{K}))^2 \text{ et } \forall C \in \mathcal{M}_{q,r}(\mathbb{K}) \ (A+B) \times C = A \times C + B \times C \end{cases}$$

Propriété 4 : $\forall \lambda \in \mathbb{K}, \ \forall (A,B) \in \mathcal{M}_{p,q}(\mathbb{K}) \times \mathcal{M}_{q,r}(\mathbb{K})$ on a :

$$(\lambda.A) \times B = \lambda.(A \times B)$$

Remarque : Le produit matriciel n'est pas un produit commutatif et ce même si il peut dans certains cas s'effectuer dans les deux sens. Soit $A \in \mathcal{M}_{p,q}(\mathbb{K})$ il y a deux éléments neutres pour A avec la loi $\times$:

1) l'élément neutre à gauche est la matrice carrée d'ordre p notée :

$$I_p = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ c'est à dire } I_p \times A = A.$$

2) l'élément neutre à droite est la matrice carrée d'ordre q notée :

$$I_q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ c'est à dire } A \times I_q = A.$$

On peut remarquer que I_p est la matrice de Id_E et I_q celle de Id_F (exprimée dans une base quelconque). Seul quand $p = q$ que l'on notera n, on peut réellement parler d'élément neutre car I_n est élément neutre à gauche et à droite et appartient au même ensemble que A étant $\mathcal{M}_n(\mathbb{K})$.

Définition : Soit $f \in \mathcal{L}(E,F)$, $\mathcal{B} = (e_1, \cdots, e_q)$ une base de E et $\mathcal{B}' = (f_1, \cdots, f_p)$ une base de F. Soit $x \in E$ tel que $x = \sum_{i=1}^{q} x_i e_i$ alors on lui associe le vecteur colonne $X = \begin{pmatrix} x_1 \\ \vdots \\ x_q \end{pmatrix} \in \mathcal{M}_{q,1}(\mathbb{K})$.

Au vecteur $f(x) = \sum_{j=1}^{p} y_j f_j$ on associe le vecteur $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_p \end{pmatrix} \in \mathcal{M}_{p,1}(\mathbb{K})$ et soit $A = M_{\mathcal{B},\mathcal{B}'} f = (a_{i,j})_{p,q} \in \mathcal{M}_{p,q}(\mathbb{K})$. On peut donc écrire une équivalence entre la définition analytique de f et une équation matricielle de f suivante :

définition analytique de $f \Leftrightarrow$ équation matricielle de f

$$\begin{cases} y_1 = a_{1,1}f_1 + a_{2,1}f_2 + \cdots + a_{p,1}f_p \\ \vdots \\ y_i = a_{1,i}f_1 + a_{2,i}f_2 + \cdots + a_{p,i}f_p \\ \vdots \\ y_q = a_{1,q}f_1 + a_{2,q}f_2 + \cdots + a_{p,q}f_p \end{cases} \Leftrightarrow \begin{pmatrix} y_1 \\ \vdots \\ y_p \end{pmatrix} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,q} \\ \vdots & \ddots & \vdots \\ a_{p,1} & \cdots & a_{p,q} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_q \end{pmatrix} \Leftrightarrow Y = AX$$

2.5. Ensemble $\mathcal{M}_n(\mathbb{K})$, les matrices carrées d'ordre n.

Théorème : $(\mathcal{M}_n(\mathbb{K}), +\times)$ est un anneau non commutatif d'élément neutre $0_{\mathcal{M}_n(\mathbb{K})} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$ et d'élément unité $I_n = 1_{\mathcal{M}_n(\mathbb{K})} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Remarque : Soit $(A,B) \in (\mathcal{M}_n(\mathbb{K}))^2$ tel que A et B commutent alors $\forall n \in \mathbb{N}^*$ on a les identités remarquables suivantes :

$$(A+B)^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} A^k \times B^{n-k}$$

$$A^n - B^n = (A-B) \times \left(\sum_{k=0}^{n-1} A^{n-1-k} \times B^k \right)$$

$$A^{2n+1} + B^{2n+1} = (A+B) \times \left(\sum_{k=0}^{2n} (-1)^k A^{2n-k} \times B^k \right)$$

Théorème d'isomorphisme :

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n et $\mathcal{B}$ une base de E.
Alors $\varphi : \begin{array}{ccc} \mathcal{L}(E) & \to & \mathcal{M}_n(\mathbb{K}) \\ f & \mapsto & M_{\mathcal{B}} f \end{array}$ est un isomorphisme d'anneau et d'espace vectoriel.

Remarque : φ n'est pas canonique et dépend de la base $\mathcal{B}$, il existe un isomorphisme canonique $\psi : \begin{array}{ccc} \mathcal{L}(\mathbb{K}^n) & \to & \mathcal{M}_n(\mathbb{K}) \\ f & \mapsto & M_{\mathcal{B}_n} f \end{array}$ avec $\mathcal{B}_n$ la base canonique de $\mathbb{K}^n$.

Définition : Soit $A \in \mathcal{M}_n(\mathbb{K})$, on dit que A est inversible si $\exists B \in \mathcal{M}_n(\mathbb{K})$ telle que $BA = I_n = AB$, et alors on notera $B = A^{-1}$.

Théorème : Soit $\mathcal{B}$ une base de E, $f \in \mathcal{L}(E)$ et $A = M_{\mathcal{B}} f$ alors :

$$A \text{ inversible} \Leftrightarrow f \in GL(E).$$

Définition : On notera $GL_n(\mathbb{K})$ l'ensemble des matrices inversibles.

Théorème d'isomorphisme :

$$(GL_n(\mathbb{K}), \times) \text{ est isomorphe à } (GL(E), \circ).$$

Pour toute base $\mathcal{B}$ de E, l'application $\varphi : \begin{array}{ccc} GL(E) & \to & GL_n(\mathbb{K}) \\ f & \mapsto & M_{\mathcal{B}} f \end{array}$ réalise cette relation isomorphisme.

Remarque : φ n'est pas canonique et dépend de la base $\mathcal{B}$, il existe un isomorphisme canonique $\psi : \begin{array}{ccc} GL(\mathbb{K}^n) & \to & GL_n(\mathbb{K})^n \\ f & \mapsto & M_{\mathcal{B}_n} f \end{array}$ avec $\mathcal{B}_n$ la base canonique de $\mathbb{K}^n$.

2.6. Matrice de changement de base

Définition : Soit $\mathcal{B} = (e_1, \cdots, e_p)$ une base de E et $(u_1, \cdots, u_q)$ une famille de vecteurs de E, avec $u_j = \sum_{i=1}^{p} a_{i,j} e_i$.

Alors on appelle matrice de la famille u_j relativement à la base $\mathcal{B}$ la matrice $A = (a_{i,j})_{p,q}$.

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,q} \\ a_{2,1} & a_{2,2} & & a_{2,q} \\ \vdots & & \ddots & \vdots \\ a_{p,1} & a_{p,2} & \cdots & a_{p,q} \\ \uparrow & \uparrow & & \uparrow \\ u_1 & u_2 & \cdots & u_q \end{pmatrix} \begin{matrix} \\ \leftarrow e_1 \\ \leftarrow e_2 \\ \vdots \\ \leftarrow e_p \\ \\ \end{matrix}$$

Définition : Soient $\mathcal{B}$ et $\mathcal{B}'$ deux base de E. On appelle matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$ la matrice de la famille $\mathcal{B}'$ relativement à la base $\mathcal{B}$ et on la note $M_{\mathcal{B}}\mathcal{B}'$.

Remarques : 1) $M_{\mathcal{B}}\mathcal{B}' = M_{\mathcal{B}',\mathcal{B}}(Id_E)$

2) $M_{\mathcal{B}}\mathcal{B} = I_n$

3) $M_{\mathcal{B}}\mathcal{B}'$ est la matrice dans la base B de l'unique endomrphisme f de E qui envoie $\mathcal{B}$ sur $\mathcal{B}'$, c'est à dire tel que $f(\mathcal{B}) = \mathcal{B}'$.

4) Soit $x \in E$ de coordonnées $(x_1, \cdots, x_n)$ dans la base $\mathcal{B}$ de E et de coordonnées $(x'_1, \cdots, x'_n)$ dans la base $\mathcal{B}'$ de E.
Si on pose $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $X' = \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}$ et $P = M_{\mathcal{B}}\mathcal{B}'$ alors on a :

$$X = PX'$$

Ou alors en notation moins compacte si l'on pose $x_{\mathcal{B}}$ le vecteur colonne correspondant à x dans la base $\mathcal{B}$ alors on a :

$$x_{\mathcal{B}} = M_{\mathcal{B}}\mathcal{B}' x_{\mathcal{B}'}$$

Théorème : Soit $P = M_{\mathcal{B}}\mathcal{B}'$ avec $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E. Alors P est inversible et $P^{-1} = M_{\mathcal{B}'}\mathcal{B}$.
Réciproquement toute matrice inversible est une matrice de changement de base, de plus pour toute matrice P inversible et toute base $\mathcal{B}$ il existe une unique base $\mathcal{B}'$ telle que $P = M_{\mathcal{B}}\mathcal{B}'$.

Théorème de changement de base : Soit $f \in \mathcal{L}(E,F)$ avec dim $E = q$ et dim $F = p$, sooient $\mathcal{B}_1$ et $\mathcal{B}'_1$ deux bases de E, soient $\mathcal{B}_2$ et $\mathcal{B}'_2$ deux bases de F, si on pose $A = M_{\mathcal{B}_1,\mathcal{B}_2}f$ et $A' = M_{\mathcal{B}'_1,\mathcal{B}'_2}f$, ainsi que $P = M_{\mathcal{B}_1}\mathcal{B}'_1$ et $Q = M_{\mathcal{B}_2}\mathcal{B}'_2$ alors :

$$A' = Q^{-1}AP$$

Ou alors en notation moins compacte :

$$M_{\mathcal{B}'_1,\mathcal{B}'_2}f = M_{\mathcal{B}'_2}\mathcal{B}_2 \times M_{\mathcal{B}_1,\mathcal{B}_2}f \times M_{\mathcal{B}_1}\mathcal{B}'_1$$

Pour un endomorphisme f de E, $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E, on pose $A = M_{\mathcal{B}}f$ et $A' = M_{\mathcal{M}'}f$ ainsi que $P = M_{\mathcal{B}}\mathcal{B}'$ alors on a :

$$A' = P^{-1}AP$$

Ou alors en notation moins compacte :

$$M_{\mathcal{B}'}f = M_{\mathcal{B}'}\mathcal{B} \times M_{\mathcal{B}}f \times M_{\mathcal{B}}\mathcal{B}'.$$

Réciproquement, soient $(A,C) \in (\mathcal{M}_{p,q}(\mathbb{K}))^2$ et $(P,Q) \in GL_q(\mathbb{K}) \times GL_p(\mathbb{K})$ telles que $C = Q^{-1}AP$ alors A et C sont les matrcie d'une même aplication linéaire exprimées dans des bases différentes.

Cas d'un endomorphisme, soient $(A,C) \in (\mathcal{M}_n(\mathbb{K}))^2$ et $P \in GL_n(\mathbb{K})$ telles que $C = P^{-1}AP$ alors A et C sont les matrices d'un même endomorphisme exprimées dans une base différente.

2.7. Rang d'une matrice

Définition : On appelle rang d'une matrice $A \in \mathcal{M}_{q,p}(\mathbb{K})$ le rang de l'unique application linéaire $f \in \mathcal{L}(\mathbb{K}^p, \mathbb{K}^q)$. dont A est la matrice relativement aux bases canoniques B_q et B_p. On note rg A =rg f.

Remarque : Le rang de A est aussi celui de ses vecteurs colonnes, ou de ses vecteurs lignes.

Théorème : Le rang d'une application $f \in \mathcal{L}(E,F)$ est égal au rang de sa matrice A relativement à des bases de $\mathcal{B}$ de E et $\mathcal{B}'$ de F quelconques.

Théorème : Soit $A \in \mathcal{M}_{q,p}(\mathbb{K})$ alors A est de rang r si et seulement si A est de la forme $A = U \times J_r \times V$ avec $(U,V) \in GL_q(\mathbb{K}) \times GL_p(\mathbb{K})$ et $J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

2.8. Matrices particulières

Définition : On dit que la matrice $A \in \mathcal{M}_n(\mathbb{K})$ est diagonale si $\forall (i,j) \in \{1, \cdots, n\}^2,\ i \neq j \Rightarrow a_{i,j} = 0$.

Proposition : L'ensemble des matrices diagonales $\mathcal{D}_n(\mathbb{K})$ de $\mathcal{M}_n(\mathbb{K})$ avec n fixé est un sous-espace vectoriel et un sous-anneau de $\mathcal{M}_n(\mathbb{K})$.

Définition : On appelle matrice scalaire toute matrice $\lambda.I_n$ avec $\lambda \in \mathbb{K}$, $\lambda.I_n$ est la matrice de $\lambda.Id_E$ et ce dans n'importe qu'elle base.

Définition : On dit que la matrice $A \in \mathcal{M}_n(\mathbb{K})$ est triangulaire supérieure si $\forall (i,j) \in \{1, \cdots, n\}^2,\ i > j \Rightarrow a_{i,j} = 0$
De même on dit que la matrice $A \in \mathcal{M}_n(\mathbb{K})$ est triangulaire inférieure si $\forall (i,j) \in \{1, \cdots, n\}^2,\ i < j \Rightarrow a_{i,j} = 0$

Proposition : L'ensemble des matrices triangulaires supérieures $TSup_n(\mathbb{K})$ et l'ensemble des matrices inférieures $TInf_n(\mathbb{K})$ de $\mathcal{M}_n(\mathbb{K})$ avec n fixé sont des sous-espaces vectoriels et des sous-anneaux de $\mathcal{M}_n(\mathbb{K})$.

Remarque : $TSup_n(\mathbb{K}) \cap TInf_n(\mathbb{K}) = \mathcal{D}_n(\mathbb{K})$.

Définition : Soit $A = (a_{i,j})_{p,q} \in \mathcal{B}_{p,q}(\mathbb{K})$ alors on appelle transposée de A la matrice noté ${}^tA = (b_{i,j})_{q,p}$ de $\mathcal{B}_{q,p}(\mathbb{K})$ définie par $b_{i,j} = a_{j,i}$.

Prorpiété 1 : $\forall (A,B) \in (\mathcal{B}_{p,q}(\mathbb{K}))^2,\ {}^t(A+B) = {}^tA +^t B$

Prorpiété 2 : $\forall A \in \mathcal{B}_{p,q}(\mathbb{K})$ et $\forall \lambda \in \mathbb{K},\ {}^t(\lambda.A) = \lambda.{}^tA$

Propriété 3 : l'application $\psi : \begin{array}{ccc} \mathcal{M}_{p,q}(\mathbb{K}) & \to & \mathcal{M}_{p,q}(\mathbb{K}) \\ A & \mapsto & {}^tA \end{array}$ est un isomorphisme d'espace vectoriel. De plus si $p = q = n$ alors on a l'application $\psi : \begin{array}{ccc} \mathcal{M}_n(\mathbb{K}) & \to & \mathcal{M}_n(\mathbb{K}) \\ A & \mapsto & {}^tA \end{array}$ qui est un automorphisme d'espace vectoriel.

Propriété 4 : $\forall (A,B) \in \mathcal{M}_{p,q}(\mathbb{K}) \times \mathcal{M}_{q,r}(\mathbb{K}),\ {}^t(A \times B) = {}^tB \times^t A$.

Propritété 5 : $\forall A \in \mathcal{M}_n(\mathbb{K}),\ A \in GL_n(\mathbb{K}) \Rightarrow {}^tA \in GL_n(\mathbb{K})$ et de plus

$$({}^tA)^{-1} =^t (A^{-1})$$

Définition : $A \in \mathcal{M}_n(\mathbb{K})$ est dite symétrique si ${}^tA = A$ équivalent à $\forall (i,j) \in \{1, \cdots, n\}\ a_{i,j} = a_{j,i}$.

On note l'ensemble des matrice symétrique de la forme $\mathcal{S}_n(\mathbb{K})$

Définition : $A \in \mathcal{M}_n(\mathbb{K})$ est dite antisymétrique si ${}^tA = -A$ équivalent à $\forall (i,j) \in \{1, \cdots, n\}\ a_{i,j} = -a_{j,i}$. On voit alors que les termes de la diagonales sont nuls.
On note l'ensemble des matrices antisymétrique de la forme $\mathcal{A}_n(\mathbb{K})$.

Théorème : $\mathcal{S}_n(\mathbb{K})$ et $\mathcal{A}_n(\mathbb{K})$ sont deux sous espaces vectoriels de $\mathcal{M}_n(\mathbb{K})$, de plus ils sont supplémentaires $\Leftrightarrow \mathcal{S}_n(\mathbb{K}) \oplus \mathcal{A}_n(\mathbb{K}) = \mathcal{M}_n(\mathbb{K})$

2.9. Operation élémentaire sur les lignes et les colonnes d'une matrice

Définition : On appelle opération élémentaire toute opération sur les lignes ou les colonnes du type :

1) Addition d'un multiple d'une ligne à une autre :

$$L_i \leftarrow L_i + \alpha.L_j \text{ avec } j \neq i$$

2) Addition d'un multiple d'une colonne à une autre :

$$C_i \leftarrow C_i + \alpha.C_j \text{ avec } j \neq i$$

Ces deux opérations reviennent à multiplier à gauche pour les lignes et droite pour les colonnes par une certaine matrice $P_{\alpha,i,j}$ inversible d'inverse $P_{-\alpha,i,j}$ avec :

$$P_{\alpha,i,j} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & & \vdots \\ \vdots & \ddots & 1 & \cdots & \alpha & & \vdots \\ \vdots & & \ddots & \ddots & \vdots & & \vdots \\ \vdots & & & \ddots & 1 & \ddots & \vdots \\ \vdots & & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix} \leftarrow \text{ligne } i$$

$$\uparrow$$

$$\text{colonne } j$$

3) Echange de deux lignes :

$$i \neq j, L_i \leftrightarrow L_j$$

4) Echange de deux colonnes :

$$i \neq j, C_i \leftrightarrow C_j$$

Ces deux opérations reviennent à multiplier à gauche pour les lignes et droite pour les colonnes par une certaine matrice $P_{i,j}$ inversible d'inverse elle même avec :

$$P_{i,j} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & & \vdots \\ \vdots & \ddots & 0 & \cdots & 1 & & \vdots \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ \vdots & & 1 & \cdots & 0 & \ddots & \vdots \\ \vdots & & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix} \begin{matrix} \\ \\ \leftarrow \text{ligne } i \\ \\ \\ \leftarrow \text{ligne } j \\ \\ \end{matrix}$$

$$\begin{matrix} & & \uparrow & & \uparrow & & \\ & & \text{colonne } i & & \text{colonne } j & & \end{matrix}$$

5) Multiplication d'une ligne par un scalaire $\lambda \neq 0$:

$$L_i \leftarrow \lambda . L_i$$

6) Multiplication d'une colonne par un scalaire $\lambda \neq 0$:

$$C_i \leftarrow \lambda . C_i$$

Ces deux opérations reviennent à multiplier à gauche pour les lignes et droite pour les colonnes par une certaine matrice $P_{\alpha,i}$ inversible d'inverse $P_{\frac{1}{\alpha},i}$ avec :

$$P_{\alpha,i} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & & & \vdots \\ \vdots & & \alpha & & \vdots \\ \vdots & & & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} \leftarrow \text{ligne } i$$

Proposition : Soit $A \in GL_n(\mathbb{K})$ donc $A \times A^{-1} = I_n$. On effectue des opérations élémentaires comme celles précédentes, d'une manière à ramener A en I_n.

Si par exemple on arrive a avoir :

$$P_p \times \cdots P_1 \times A \times P'_1 \times \cdots \times P'_q = I_n$$

Où les P_i sont des opérations élémentaires sur les lignes et les P'_i des opérations sur les colonnes alors on trouve :
$P_p \times \cdots P_1 \times A \times P'_1 \times \cdots \times P'_q = I_n$

$A = {P_1}^{-1} \times \cdots \times {P_p}^{-1} \times I_n \times {P'_q}^{-1} \times \cdots \times {P'_1}^{-1}$.

donc

$A^{-1} = P'_1 \times \cdots \times P'_q \times I_n \times P_p \times \cdots \times P_1$.

Pour plus de logique :

$A^{-1} = (I_n \times P'_1 \times \cdots \times P'_q) \times (P_p \times \cdots \times P_1 \times I_n)$.

On applique donc les transformations sur les colonnes à I_n, on applique les transformations sur les lignes à part à I_n et on multiplie le premier résultat avec le second, le premier à gauche et le second à droite.

On remarque que si on ne fait que des opérations sur les lignes ou seulement sur les colonnes alors on effectue simultanement les mêmes à I_n pour arriver à A^{-1}.

Théorème : Le rang d'une matrice reste inchangé par opérations élémentaires.

Remarque : Pour trouver le rang de A on tente de ramener A par opérations élémentaires jusqu'à une matrice de la forme $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$ ou plus rapidement à une matrice de la forme $\begin{pmatrix} TS_r & 0 \\ 0 & 0 \end{pmatrix}$ ou $\begin{pmatrix} TI_r & 0 \\ 0 & 0 \end{pmatrix}$ avec TS_r triangulaire supérieure et TI_r triangulaire inférieur et alors r sera le rang de A.

CHAPITRE VII : Déterminant

1. Groupe symétrique

1.1. Groupe $(\mathfrak{S}_n, \circ)$

Définition : $\mathfrak{S}_n$ est l'ensemble des bijections de $\{1, \cdots, n\}$, appelées aussi permutations.

Proposition : $(\mathfrak{S}_n, \circ)$ est un groupe non commutatif.

1.2. Orbites

Définition : Soit $s \in \mathfrak{S}_n$ et $a \in \{1, \cdots, n\}$. On appelle orbite de a l'ensemble des éléments $x \in \{1, \cdots, n\}$ tel que $\exists k \in \mathbb{Z}$ / $x = s^k(a)$ soit

$$O(a) = \left\{ x \in \{1, \cdots, n\} \text{ / } \exists k \in \mathbb{Z}, x = s^k(a) \right\}$$

On appelle longueur de l'orbite de a le cardinal de $O(a)$.
On définit par récurrence :

$$\text{si } k > 0,\ s^k = \underbrace{s \circ \cdots \circ s}_{k \text{ fois}}$$

$$\text{si } k < 0,\ s^k = \underbrace{s^{-1} \circ \cdots \circ s^{-1}}_{-k \text{ fois}}$$

$$\text{si } k = 0 \text{ alors } s^k = s^0 = Id_{\{1,\cdots,n\}}$$

Remarque : $O(a) = \left\{ a \right\} \Leftrightarrow s(a) = a$.

1.3. Décomposition d'une permutation en produit de cycles

Définition : On appelle cycle toute permutation ne comptant qu'une orbite de plus de 2 éléments. Et on appelle ordre du cyle la longueur de cette orbite. On note $(i_1, \cdots, i_r)$ le cycle de longueur r tel que $\forall k \in \{1, \cdots, r-1\},\ s(i_k) = i_{k+1}$,$s(i_r) = i_1$ et tel que tout autre élément soit un point fixe de s.

Théorème de décomposition : Toute permutation se décompose en un produit commutatif de cycles.

1.4. Décomposition en produit de transposition

Définition : On appelle transposition tout cycle d'ordre 2. On note (i, j) la transposition qui échange i et j distincts.

Théorème de décomposition : Toute permutation se décompose en produit non commutatif de transposition.

1.5. Signature d'une permutation

Définition : Soit $s \in \mathfrak{S}_n$, on appelle signature de la permutation s le nombre noté $\varepsilon(s)$ égal à :

$$\varepsilon(s) = \prod_{i<j} \frac{s(j) - s(i)}{j - i}$$

Proposition : $\forall s \in \mathfrak{S}_n$, $\varepsilon(s) = \pm 1$.

Théorème : La signature d'une transposition est égale à -1.

Théorème : $\varepsilon : \begin{array}{ccc} \mathfrak{S}_n & \to & \{-1, 1\} \\ s & \mapsto & \varepsilon(s) \end{array}$ est un morphisme de groupe de $(\mathfrak{S}_n, \circ)$ dans le groupe $(\{-1, 1\}, \times)$.

Proposition : Soit $s \in \mathfrak{S}_n$, $\varepsilon(s) = (-1)^k$ si s est le produit de k transpositions, et est unique modulo 2.

Définition : On appelle groupe alterné d'ordre n le sous-groupe de $\mathfrak{S}_n$ noté $\mathfrak{A}_n$ défini par $\mathfrak{A}_n = ker\ \varepsilon = \left\{ s \in \mathfrak{S}_n \ / \ \varepsilon(s) = 1 \right\}$.

2. Applications multilinéaire

2.1. Définition

Définition : Soient $E_1, \cdots, E_n$ et F des $\mathbb{K}$-espaces vectoriels. On dit que l'application f de $E_1 \times \cdots \times E_n$ dans F est n-linéaire si $\forall i \in \{1, \cdots, n\}$, et $\forall (u_1, \cdots, u_{i-1}, u_{i+1}, \cdots, u_n) \in E_1 \times \cdots \times E_{i-1} \times E_{i+1} \times \cdots \times E_n$, l'application : $\begin{array}{ccc} E_i & \to & F \\ u & \mapsto & f(u_1, \cdots, u_{i-1}, u, u_{i+1}, \cdots, u_n) \end{array}$ est linéaire.

Ne pas confondre multilinéarité et linéarité sur l'espace produit.

Définition : On dit que l'application n-linéaire f de $E_1 \times \cdots \times E_n$ dans F est symétrique si $\forall (u_1, \cdots, u_n) \in E_1 \times \cdots \times E_n$ et $\forall s \in \mathfrak{S}_n$ on a :

$$f(u_{s(1)}, \cdots, u_{s(n)}) = f(u_1, \cdots, u_n)$$

Définition : On dit que l'application n-linéaire f de $E_1 \times \cdots \times E_n$ dans F est antisymétrique si $\forall (u_1, \cdots, u_n) \in E_1 \times \cdots \times E_n$ et $\forall s \in \mathfrak{S}_n$ on a :

$$f(u_{s(1)}, \cdots, u_{s(n)}) = \varepsilon(s) f(u_1, \cdots, u_n)$$

Définition : On dit que l'application n-linéaire f de $E_1 \times \cdots \times E_n$ dans F est alternée si $\forall (u_1, \cdots, u_n) \in E_1 \times \cdots \times E_n$ et $\forall s \in \mathfrak{S}_n$ on a :

$$\exists (i, j) \in \{1, \cdots, n\}, \text{ avec } i \neq j \text{ tel que } u_i = u_j \Rightarrow f(u_1, \cdots, u_n) = 0$$

2.2. Forme multilinéaire

Définition : Soit E un $\mathbb{K}$-espace vectoriel, une application n linéaire de E^n dans $\mathbb{K}$, est appelée forme n-linéaire sur E.

Propriété 1 : Soit f une forme n-linéaire sur E,

$$f \text{ antisymétrique} \Leftrightarrow f \text{ alternée}$$

Propriété 2 : Soit f une forme n-linéaire sur E antisymétrique. $\forall (u_1, \cdots, u_n) \in E^n$ et $\forall j \in \{2, \cdots, n\}$ on a :

$$f(u_j, u_1, \cdots, u_{j-1}, u_{j+1}, \cdots, u_n) = (-1)^{j-1} f(u_1, \cdots, u_n).$$

3. Déterminants

3.1. Déterminant de n vecteurs

Théorème : Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \geq 1$, et $\mathcal{B} = (e_1, \cdots, e_n)$ une base de E. Alors il existe une unique forme n-linéaire alternée f sur E telle que $f(e_1, \cdots, e_n) = 1$.

Définition : Soit $\mathcal{B} = (e_1, \cdots, e_n)$ une base de E, on appelle l'unique forme n-linéaire alternée f sur E telle que $f(e_1, \cdots, e_n) = 1$ déterminant dans la base $\mathcal{B}$ et notée $\det_{\mathcal{B}}$.

Définition : Si $(v_1, \cdots, v_n)$ sont des vecteurs tels que $v_j = \sum_{i=1}^{n} x_{i,j} e_i$. Alors on note sous la forme suivante :

$$\det_{\mathcal{B}}(v_1, \cdots, v_n) = \begin{vmatrix} x_{1,1} & \cdots & x_{1,n} \\ \vdots & \ddots & \vdots \\ x_{n,1} & \cdots & x_{n,n} \end{vmatrix}$$

Proposition : Pour calculer le déterminant suivant $\det_{\mathcal{B}}(v_1, \cdots, v_n) = \begin{vmatrix} x_{1,1} & \cdots & x_{1,n} \\ \vdots & \ddots & \vdots \\ x_{n,1} & \cdots & x_{n,n} \end{vmatrix}$, on va mettre en place un procédé de récurrence. On appelle $\Delta_{i,j}$ le déterminant extrait de $\det_{\mathcal{B}}(v_1, \cdots, v_n)$ auquel on a retiré la $i^{ème}$ ligne et la $j^{ème}$ colonne. On a donc alors la relation de récurrence suivante :

$$\det_{\mathcal{B}}(v_1, \cdots, v_n) = \sum_{i=1}^{n} (-1)^{i+j} x_{i,j} \Delta_{i,j}$$

appelée développement par rapport à la $j^{ème}$ colonne (j fixée).

Ou encore :

$$\det_{\mathcal{B}}(v_1, \cdots, v_n) = \sum_{j=1}^{n} (-1)^{i+j} x_{i,j} \Delta_{i,j}$$

appelée développement par rapport à la $i^{ème}$ ligne (i fixée).

3.2. Déterminant d'une matrice carrée

Définition : On appelle déterminant de la matrice carrée d'ordre n, $A = (a_{i,j})_n \in \mathcal{M}_n(\mathbb{K})$, le déterminant des vecteurs colonnes de A pris comme vecteurs de $\mathbb{K}^n$ et exprimés dans la base canonique $\mathcal{B}_n$, donc

$$\det A = \det_{\mathcal{B}}(C_1, \cdots, C_n) = \begin{vmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{vmatrix}$$

De même on le calcule en développant par rapport aux colonnes ou aux lignes avec les formules :

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{i,j} \det(A_{i,j}) \text{ par rapport à la } j^{ème} \text{ colonne}$$

ou alors :

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j} \det(A_{i,j}) \text{ par rapport à la } i^{ème} \text{ ligne.}$$

où $A_{i,j}$ est la matrice carrée d'ordre $n-1$ obtenue en ôtant la $i^{ème}$ ligne et la $j^{ème}$ colonne.

Les éléments $det(A_{i,j})$ sont appelées les déterminants mineurs de A. La valeur $(-1)^{i+j} \det(A_{i,j})$ est appelée cofacteur de $a_{i,j}$.

3.3. Déterminant d'une matrice triangulaire

Proposition : Soit $A = (a_{i,j})_n \in \mathcal{M}_n(\mathbb{K})$ une matrice triangulaire supérieure ou inférieure. Alors si on développe toujours par rapport à la $1^{ère}$ colonne si A est triangulaire supérieure, ou alors par rapport à la $1^{ère}$ ligne si A est triangulaire inférieure alors on trouve : $\det A = \prod_{i=1}^{n} a_{i,i}$.

3.4. Action du groupe symétrique

Théorème 1 : Soit $\mathcal{B}$ une base de E alors $\det_{\mathcal{B}}$ est antisymétrique
$\Leftrightarrow \forall (u_1, \cdots, u_n) \in E^n$ et $\forall s \in \mathfrak{S}_n$ on a :

$$\det_{\mathcal{B}}(u_{s(1)}, \cdots, u_{s(n)}) = \varepsilon(s) \det_{\mathcal{B}}(u_1, \cdots, u_n)$$

Théoreme 2 : Soit $\mathcal{B} = (e_1, \cdots, e_n)$ une base de E et les vecteurs $(u_1, \cdots, u_n) \in E^n$ tels que $u_j = \sum_{i=1}^{n} x_{i,j} e_i$ alors :

$$\det_{\mathcal{B}}(u_1, \cdots, u_n) = \sum_{s \in \mathfrak{S}_n} \varepsilon(s) \prod_{i=1}^{n} x_{s(i),i}$$

Théorème 3 : Soit $A \in \mathcal{M}_n(\mathbb{K})$ alors $\det({}^tA) = \det(A)$.

4. Applications du déterminant

4.1. Indépendance linéaire de n vecteurs

Théorème 1 : Soit E de dimension n, $\mathcal{B} = (e_1, \cdots, e_n)$ une base de E et les n vecteurs $(v_1, \cdots, v_n) \in E^n$. Alors :

$$(v_1, \cdots, v_n) \text{ liée} \Leftrightarrow \det_{\mathcal{B}}(v_1, \cdots, v_n) = 0$$

$$(v_1, \cdots, v_n) \text{ libre} \Leftrightarrow \det_{\mathcal{B}}(v_1, \cdots, v_n) \neq 0$$

4.2. Changement de base de calcul d'un déterminant

Théorème 2 : Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E alors :

$$\forall (v_1, \cdots, v_n) \in E^n,\ \det_{\mathcal{B}'}(v_1, \cdots, v_n) = \frac{1}{\det_{\mathcal{B}} \mathcal{B}'} \det_{\mathcal{B}}(v_1, \cdots, v_n)$$

4.3. Déterminant d'un endormorphisme

Théorème 3 : Soit $f \in \mathcal{L}(E)$ alors $\exists! K \in \mathbb{K}$ tel que $\forall \mathcal{B}$ une base de E et $\forall (v_1, \cdots, v_n) \in E^n$, on ait :

$$\det_{\mathcal{B}}(f(v_1), \cdots, f(v_n)) = K \det_{\mathcal{B}}(v_1, \cdots, v_n)$$

Définition : On appelera déterminant de l'endormorphisme f la constante K précédemment citée et on le note $\det f$.

Propriété 1 : Soit $f \in \mathcal{L}(E)$ et $\mathcal{B}$ une base de E alors $\det M_{\mathcal{B}} f = \det f$

Propriété 2 : Soit $(f, g) \in (\mathcal{L}(E))^2$ alors $\det(g \circ f) = \det g \times \det f$

Propriété 3 : Soit $(A, B) \in (\mathcal{L}_n(\mathbb{K}))^2$, alors $\det(A \times B) = \det A \times \det B$.

Propriété 4 : Soit $A \in \mathcal{M}_n(\mathbb{K})$ alors :

$$A \text{ inversible} \Leftrightarrow \det A \neq 0$$

Dans ce cas alors $\det(A^{-1}) = \dfrac{1}{\det A}$

Propriété 5 : $\psi : \begin{array}{ccc} GL_n(\mathbb{K}) & \to & \mathbb{K}^* \\ A & \mapsto & \det A \end{array}$ est un morphisme de groupe du groupe $(GL_n(\mathbb{K}), \circ)$ dans le groupe $(\mathbb{K}^*, \times)$.

4.4. Calcul de l'inverse d'une matrice

Définition : On appelle comatrice de A la matrice notée com A égale à com $A = (\det(A_{i,j}))$ avec $A_{i,j}$ la sous-matrice d'ordre $n-1$ obtenue en ôtant la $i^{ème}$ ligne et la $j^{ème}$ colonne.

Théorème : Soit $A \in GL_n(\mathbb{K})$ alors $A^{-1} = \dfrac{1}{\det A}\ {}^t\text{com}A$.

4.5. Règles de calcul

Proposition : 1) Soit $\lambda \in \mathbb{K}$, et $A \in \mathcal{M}_n(\mathbb{K})$ alors $\det(\lambda.A) = \lambda^n \det A$

2) $\det(A + B) \neq \det A + \det B$ en général.

3) Le déterminant change de signe si on échange deux colonnes ou 2 lignes.

4) Si 2 colonnes ou deux lignes sont proportionnelles alors le déterminant est nul.

5) On peut ajouter à une colonne (resp à une ligne) une combinaison linaire des autres colonnes (resp lignes) dans changer la valeur du déterminant.

CHAPITRE VIII : Systèmes linéaires