DUMI2E *2007-2008*

Notes de cours Algèbre 1

Ce polycopié a été écrit par Jérôme RENAULT. Le chapitre 4 vient des notes de cours de Françoise DIBOS, le chapitre 5 de celles de Pierre CARDALIAGUET.

BIBLIOGRAPHIE

- François LIRET et Dominique MARTINAIS : Mathématiques pour le DEUG. Algèbre 1ère année. L1. Cours et exercices avec solutions, DUNOD.

- Jean-Hervé COHEN et Nathalie CLEIREC : Les aventures de l'irréductible mathématix, Ellipses.

- Geneviève PONS et Suzel ROVERATO : Aide mémoire de mathématiques, Ellipses.

On pourra aussi consulter tout cours d'algèbre pour premier cycle universitaire.

CHAPITRE 1

NOTIONS DE BASE

I. ENSEMBLES

Inclusion

On dit que l'ensemble A est inclus dans l'ensemble B, ou que A est un sous-ensemble ou une partie de B et on note $A \subset B$ si tout élément de A est un élément de B :

$$\forall x \in A, x \in B$$

L'ensemble vide est inclus dans tout ensemble : $\emptyset \subset A$.

E étant un ensemble, l'ensemble des parties de E est noté $\mathcal{P}(E)$.
Les opérations classiques sur $\mathcal{P}(E)$ sont :
- le complémentaire d'une partie A dans E noté $\complement_E(A)$ ou A^c s'il n'y a pas d'ambiguïté ;
- l'union de deux parties A et B, $A \cup B$;
- l'intersection de deux parties A et B, $A \cap B$;
- la différence de deux parties $A \setminus B$, qui vaut $A \cap \complement_E(B)$.

Propriétés des opérations sur les parties d'un ensemble

Associativité : $A \cup (B \cup C) = (A \cup B) \cup C$ et $A \cap (B \cap C) = (A \cap B) \cap C$.
Distributivité de $\cap$ par rapport à $\cup$: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
Distributivité de $\cup$ par rapport à $\cap$: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
Lois de Morgan : $\complement_E(A \cap B) = \complement_E(A) \cup \complement_E(B)$ et $\complement_E(A \cup B) = \complement_E(A) \cap \complement_E(B)$.

Produit cartésien

A partir de deux ensembles A et B, on crée un nouvel ensemble noté $A \times B$, dont les éléments sont les couples (a, b) constitués d'un élément a de A et d'un élément b de B dans cet ordre.

$$A \times B = \{\ (x, y),\ x \in A \text{ et } y \in B\ \}.$$

On peut généraliser cette construction à un nombre fini d'ensembles :

$A_1 \times A_2 \times \cdots \times A_n$ dont les éléments sont des n-uplets : $(a_1, a_2 \cdots, a_n)$.
$A \times A$ se note A^2, $\underbrace{A \times \cdots \times A}_{n\text{fois}}$ se note A^n.

II. APPLICATIONS

E et F étant des ensembles, une application f de E vers F est un moyen d'associer à chaque élément de E un élément unique de F. On note :
$f : E \to F$
$\quad x \mapsto f(x)$
$f(x)$ s'appelle l'image de x par f.
Le graphe de f est l'ensemble des couples $(x, f(x))$, c'est une partie de $E \times F$.
E s'appelle l'ensemble de départ de f. F s'appelle l'ensemble d'arrivée de f.

Image directe
Soit $f : E \to F$ et A une partie de E.
L'image (directe) de A par f est la partie de F notée $f(A)$ formée des images de tous les éléments de A. Pour $y \in F$,

$$y \in f(A) \iff \exists x \in A,\ y = f(x)\,.$$

Par exemple, si $A = \{a, b, c\}$, $f(A) = \{f(a), f(b), f(c)\}$.

Image réciproque
Soit $f : E \to F$ et y un élément de F, un élément x de E tel que $f(x) = y$ s'appelle un antécédent de y. L'image réciproque d'une partie B de F par f est la partie de E notée $f^{-1}(B)$ formée des antécédents de tous les éléments de B. Pour $x \in E$,

$$x \in f^{-1}(B) \iff f(x) \in B\,.$$

Proposition : Soit $f : E \longrightarrow F$ une application. Soient A et A' des parties de E, et B et B' des parties de F. Alors :

$A \subset f^{-1}(f(A))$	$f(f^{-1}(B)) \subset B$
$f(A \cup A') = f(A) \cup f(A')$	$f(A \cap A') \subset f(A) \cap f(A')$
$f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$	$f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B')$

Composée de deux applications
$f : E \to F$ et $g : F \to G$ étant des applications, on définit la composée des applications f et g par :

$$g \circ f : E \to G$$
$$x \mapsto g \circ f(x) = g(f(x))$$

Si $h : G \longrightarrow H$, alors $h \circ (g \circ f) = (h \circ g) \circ f$.

Injectivité
$f : E \to F$ est injective si chaque élément de F a au plus un antécédent dans E.
C'est équivalent à : $\forall x, x' \in E$, $(f(x) = f(x')) \implies (x = x')$.
La composée de deux applications injectives est injective.
Si $g \circ f$ est injective, alors f est injective.

Surjectivité
Une application $f : E \to F$ est surjective si chaque élément de F a au moins un antécédent dans E :

$$\forall y \in F,\ \exists x \in E,\ y = f(x).$$

C'est équivalent à : $f(E) = F$.
La composée de deux applications surjectives est surjective.
Si $g \circ f$ est surjective, alors g est surjective.

Bijectivité, application réciproque
$f : E \to F$ est bijective si chaque élément de F a exactement un antécédent dans E, ce qui revient à dire que f est injective et surjective.

$$\forall y \in F,\ \exists! x \in E,\ y = f(x).$$

On peut alors définir l'application réciproque de f, notée f^{-1}, de F vers E telle que : pour $y \in F$ et $x \in E$, $(y = f(x)) \iff (x = f^{-1}(y))$.
Si f est bijective, alors $f^{-1} \circ f = Id_E$ et $f \circ f^{-1} = Id_F$.
S'il existe une application g de F vers E telle que $g \circ f = Id_E$ et $f \circ g = Id_F$, alors f est bijective et $g = f^{-1}$.
Si g et f sont bijectives et se composent, alors $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Familles indexées
Si I est un ensemble, on appelle famille indexée par I toute application f d'ensemble de départ I.

On note la famille $f : I \to F$ plutôt par $(x_i)_{i\in I}$.
$i \mapsto f(i) = x_i$

exemple : Suite de réels : $(x_n)_{n\in\mathbb{N}}$ avec $x_n \in \mathbb{R}\ \forall n \in \mathbb{N}$. C'est une famille indexée par l'ensemble $\mathbb{N}$.

Si $I \neq \emptyset$, si E est un ensemble et pour tout i de I A_i est un sous-ensemble de E, on définit l'union, l'intersection et le produit de la famille $(A_i)_{i\in I}$.

$\bigcup_{i\in I} A_i = \{x, \exists i \in I \text{ tel que } x \in A_i\}$ (union de la famille $(A_i)_{i\in I}$)

$\bigcap_{i\in I} A_i = \{x, \forall i \in I, x \in A_i\}$ (intersection de la famille $(A_i)_{i\in I}$)

$\prod_{i\in I} A_i = \{(x_i)_{i\in I}, \forall i \in I, x_i \in A_i\}$ (produit de la famille $(A_i)_{i\in I}$)

Une famille $(A_i)_{i\in I}$ de sous-ensembles d'un ensemble E est une partition de E si :

$$E = \cup_{i\in I} A_i \qquad \text{et} \qquad A_i \cap A_j = \emptyset\ \forall i \in I, \forall j \in J \text{ t.q. } i \neq j$$

III. RELATIONS BINAIRES

Une relation binaire $\mathcal{R}$ est définie par un ensemble E et par une partie G de $E \times E$. On dit alors que $\mathcal{R}$ est une relation binaire sur E. On dit que x est en relation avec y et on note $x\,\mathcal{R}\,y$ si et seulement si $(x, y) \in G$.
Une relation est en général définie par une propriété commune aux couples (x, y), par exemple la relation $\mathcal{R}$ sur $\mathbb{R}$ telle que : $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x\,\mathcal{R}\,y \iff x - y = 1$.

Relation d'équivalence

Une relation d'équivalence $\mathcal{R}$ vérifie les trois propriétés suivantes :

- réflexivité : pour tout x de E, $x\,\mathcal{R}\,x$; on dit que $\mathcal{R}$ est réflexive ;
- symétrie : pour tous x et y de E, si $x\,\mathcal{R}\,y$ alors $y\,\mathcal{R}\,x$; on dit que $\mathcal{R}$ est symétrique ;
- transitivité : pour tous x, y et z de E, si $x\,\mathcal{R}\,y$ et $y\,\mathcal{R}\,z$, alors $x\,\mathcal{R}\,z$; on dit que $\mathcal{R}$ est transitive.

Une relation d'équivalence permet de regrouper les éléments d'un ensemble en classes d'équivalence ; la classe de l'élément a, notée $\mathcal{C}(a)$, est l'ensemble de tous les éléments x tels que $x\,\mathcal{R}\,a$, ces éléments sont dits équivalents à a.

Partition d'un ensemble en classes d'équivalence
Lorsque $\mathcal{R}$ est une relation d'équivalence sur un ensemble E, l'ensemble des classes d'équivalences est appelé ensemble quotient de E par $\mathcal{R}$, noté $E/\mathcal{R}$.
L'ensemble $E/\mathcal{R}$ possède trois propriétés remarquables :
- aucune classe d'équivalence n'est vide,
- deux classes distinctes sont disjointes,
- l'union de toutes les classes d'équivalence est l'ensemble E.

La famille $(\mathcal{C}(x))_{\mathcal{C}(x)\in E/\mathcal{R}}$ des classes d'équivalences est donc une partition de E.

Relation d'ordre
La relation binaire $\mathcal{R}$ sur E est dite antisymétrique si pour tous x et y de E :

$$x\,\mathcal{R}\,y \text{ et } y\,\mathcal{R}\,x \text{ entraîne } x = y\,.$$

$\mathcal{R}$ est une relation d'ordre si elle est réflexive, antisymétrique et transitive. On dit alors que $(E, \mathcal{R})$ est un ensemble ordonné.
Par exemple, l'inclusion entre parties d'un ensemble est une relation d'ordre.

Ordre total, ordre partiel
On note $\preceq$ une relation d'ordre sur E ; $x \preceq y$ se lit "x est plus petit que y" ou "y est plus grand que x".
L'ordre est total si deux éléments quelconques de E sont toujours comparables :

$$\forall (x, y) \in E \times E,\ x \preceq y \text{ ou } y \preceq x.$$

Dans le cas contraire, l'ordre est dit partiel.
Ainsi l'inclusion est une relation d'ordre partiel sur les parties d'un ensemble E fixé (si E a au moins 2 éléments), la relation $\leq$ est une relation d'ordre total sur $\mathbb{R}$.

Majorant, minorant
A étant une partie de E,
$x \in E$ est un majorant de A si pour tout $a \in A$, $a \preceq x$.
$y \in E$ est un minorant de A si pour tout $a \in A$, $y \preceq a$.
Une partie A de E est majorée lorsqu'elle admet un majorant, minorée lorsqu'elle admet un minorant. A est bornée si elle est à la fois majorée et minorée.

Plus grand élément, plus petit élément
S'il existe un élément de A qui soit un majorant de A, cet élément est unique et on l'appelle le plus grand élément, ou le maximum, de A ; il se note : $\max A$.

De même, si A possède un élément minorant, il est unique et s'appelle le plus petit élément, ou le minimum, de A ; on le note : $\min A$.

Borne supérieure, borne inférieure

On remarque que si M est un majorant d'une partie A, tout élément plus grand que M est également un majorant de A. Si l'ensemble des majorants de A possède un plus petit élément, c'est le plus petit majorant de A. Cet élément, lorsqu'il existe, s'appelle la borne supérieure de A et se note : $\sup A$.
On retient : la borne supérieure de A est le plus petit des majorants de A.
On définit de même la borne inférieure de A, notée $\inf A$, comme étant le plus grand des minorants de A.

Pour toute partie A d'un ensemble ordonné,

si A a un maximum, alors A a une borne supérieure et $\max A = \sup A$.
si A a un minimum, alors A a une borne inférieure et $\min A = \inf A$.

Cas particulier de l'ensemble ordonné $(\mathbb{R}, \leq)$

Toute partie non vide et majorée de $\mathbb{R}$ a une borne supérieure.
Toute partie non vide et minorée de $\mathbb{R}$ a une borne inférieure.

CHAPITRE 2

NOMBRES ENTIERS ET COMPLEXES

I. ENTIERS NATURELS

$\mathbb{N}$ est l'ensemble des entiers naturels : $\{0, 1, 2, \ldots\}$, il est muni d'une relation d'ordre totale notée $\leq$.
Dans $\mathbb{N}$, toute partie non vide possède un plus petit élément : on dit que $\mathbb{N}$ est un ensemble bien ordonné.

Récurrence
Pour démontrer par récurrence qu'une propriété dépendant de l'entier n est vraie *pour tout entier naturel* n, on procède en deux étapes :
- On démontre que la propriété est vraie pour $n = 0$.
- On suppose que la propriété est vraie pour n fixé dans $\mathbb{N}$: c'est *l'hypothèse de récurrence*, puis on démontre qu'alors la propriété est vraie pour $n + 1$.

En appelant la propriété à démontrer $P(n)$, ces deux étapes se résument ainsi :
- $P(0)$ est vraie
- Pour tout $n \in \mathbb{N}$, $(P(n) \implies P(n+1))$.

Si nécessaire, l'hypothèse de récurrence simple $P(n)$ peut être remplacée par :
- on suppose que la propriété est vraie pour tout entier naturel $k \leq n$.

Ensembles finis
Théorème : Soient n et p dans $\mathbb{N}$ tels qu'il existe une injection de $\{1, ..., n\}$ dans $\{1, ..., p\}$. Alors $n \leq p$.

Un ensemble E est fini s'il est vide ou s'il existe $n \in \mathbb{N}^*$ et une bijection de E dans $\{1, .., n\}$.
S'il existe $n \in \mathbb{N}^*$ et une bijection de E dans $\{1, .., n\}$, alors n est unique et s'appelle le cardinal ou le nombre d'éléments de E. Le cardinal de $\emptyset$ est zéro. On note $\mathrm{Card}(E)$ le cardinal de E quand E est fini.
Proposition : Soit E un ensemble fini, et F un ensemble.
1) (Il existe une bijection de E dans F) si et seulement si (F est fini et $\mathrm{Card}(F) = \mathrm{Card}(E)$).
2) Si $F \subset E$, alors F est fini et $\mathrm{Card}(F) \leq \mathrm{Card}(E)$.

3) Si E et F sont finis, alors $E \cup F$ et $E \cap F$ sont finis et :

$$\mathrm{Card}(E \cup F) + \mathrm{Card}(E \cap F) = \mathrm{Card}(E) + \mathrm{Card}(F)$$

4) Si E et F sont finis, notons $n = \mathrm{Card}(E)$ et $p = \mathrm{Card}(F)$. Alors il y a p^n applications de E dans F, il y a $n!$ bijections de E dans E, et il y a 2^n parties de E (autrement dit, $\mathrm{Card}(\mathcal{P}(E)) = 2^n$).

Ensembles infinis
Un ensemble E est dit infini s'il n'est pas fini. $\mathbb{N}$ est infini.
Un ensemble infini E est dit dénombrable s'il existe une bijection de $\mathbb{N}$ dans E (cela revient à dire que l'on peut ranger les éléments de E en une suite $(e_n)_{n\in\mathbb{N}}$ d'éléments deux à deux distincts).
$\mathbb{N}, \mathbf{Z}, \mathbb{Q}$ sont dénombrables, l'ensemble des parties de $\mathbb{N}$ n'est pas dénombrable (et est en bijection avec $\mathbb{R}$, donc $\mathbb{R}$ n'est pas dénombrable).

II. ENTIERS RELATIFS

$\mathbf{Z} = \mathbb{N} \cup -\mathbb{N} = \{..., -3, -2, -1, 0, 1, ..., 7, ...\}$.
$(\mathbf{Z}, \leq)$ est un ensemble totalement ordonné.

Division euclidienne
Théorème : Soit $(a, b) \in \mathbf{Z}^2$ avec $b \neq 0$, alors il existe un unique couple (q, r) dans $\mathbf{Z} \times \mathbf{Z}$ tel que :

$$a = bq + r \quad \text{et} \quad 0 \leq r < |b|$$

q s'appelle le quotient, r le reste de la division euclidienne de a par b.

Relation de divisibilité
Dans $\mathbf{Z}$, on dit que b divise a ou que b est un diviseur de a ou que a est un multiple de b s'il existe $q \in \mathbf{Z}$ tel que : $a = bq$. On note $b \mid a$.
La relation de divisibilité est réflexive et transitive. Sur $\mathbb{N}$, c'est une relation d'ordre partiel.

Nombres premiers
Un nombre premier est un entier $p \geq 2$ dont les seuls diviseurs dans $\mathbf{Z}$ sont $1, -1, p$ et $-p$.
Théorème : Décomposition en facteurs premiers
Tout entier $n \in \mathbf{Z}\backslash\{0, 1, -1\}$ se décompose en produit de facteurs premiers : $n = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$;

$\varepsilon \in \{+1, -1\}$ est le signe de n, $r \in \mathbb{N}^*$, $p_1, ..., p_r$ sont des nombres premiers distincts deux à deux, $\alpha_1, ..., \alpha_r$ sont des entiers strictement positifs.
De plus, ε, r et l'ensemble $\{(p_1, \alpha_1), ..., (p_r, \alpha_r)\}$ sont uniques pour l'entier n donné.

III. RATIONNELS ET REELS

$\mathbb{Q} = \{p/q, p \in \mathbf{Z}, q \in \mathbf{Z}^*\}$ est l'ensemble des nombres rationnels.
Tout rationnel non nul r admet un inverse dans $\mathbb{Q}$, c'est-à-dire qu'il existe $r' \in \mathbb{Q}$ tel que $rr' = 1$.
Tout nombre rationnel r peut s'écrire de façon unique sous la forme $r = a/b$, avec $a \in \mathbf{Z}$ et $b \in \mathbb{N}^*$ tels que a et b n'aient pas de diviseurs communs autres que 1 et -1.
$\mathbb{R}$ est l'ensemble des nombres réels.
Pour a et x réels avec $a > 0$, $a^x = \exp(x \ln a)$.

$$\mathbb{N} \subset \mathbf{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

IV. NOMBRES COMPLEXES

$$\mathbb{C} = \{x + iy, x \in \mathbb{R}, y \in \mathbb{R}\}$$

Un nombre complexe z s'écrit de façon unique $z = x + iy$ où x et y sont réels et i vérifie $i^2 = -1$.
x est la partie réelle de z, et y est la partie imaginaire de z. On note $x = \Re\mathrm{e}(z)$ et $y = \Im\mathrm{m}(z)$.

Le conjugué de $z = x + iy$ est défini par : $\bar{z} = x - iy$.
$\Re\mathrm{e}(z) = (z + \bar{z})/2, \Im\mathrm{m}(z) = (z - \bar{z})/2i$.
Le module de $z = x + iy$ est défini par : $|z| = \sqrt{x^2 + y^2}$.
On a, pour tous z et z' de $\mathbb{C}$:
$|z| = 0$ ssi $z = 0$
$z = \bar{z}$ ssi z est réel
$z\bar{z} = |z|^2$, $|\bar{z}| = |z|, |zz'| = |z||z'|$
Inégalité triangulaire : $|z + z'| \leq |z| + |z'|$
Si $z \neq 0$, z a pour inverse $z^{-1} = \frac{1}{|z|^2}\bar{z}$.

Exponentielle complexe
Pour $t \in \mathbb{R}$, $e^{it} = \cos(t) + i \sin(t)$.

$\overline{e^{it}} = e^{-it} = \dfrac{1}{e^{it}}$.
Cercle unité : $U = \{z \in \mathbb{C}, |z| = 1\} = \{e^{it}, t \in \mathbb{R}\} = \{e^{it}, t \in [0, 2\pi[\}$
Pour tous réels t et t',

$$e^{i(t+t')} = e^{it}e^{it'}$$

On retrouve bien : $\cos(t+t') = \cos t \cos t' - \sin t \sin t'$, et $\sin(t+t') = \sin t \cos t' + \sin t' \cos t$.

On définit l'exponentielle d'un nombre complexe z quelconque par : si $z = x+iy$, avec $x = \Re\mathrm{e}(z)$ et $y = \Im\mathrm{m}(z)$, $e^z = e^x e^{iy}$. Pour tous z et z' dans $\mathbb{C}$, on a alors $e^{z+z'} = e^z e^{z'}$.

Formule de *de Moivre* :
Pour tout n de $\mathbf{Z}$, $(\cos t + i\sin t)^n = \cos(nt) + i\sin(nt)$; on l'utilise notamment pour exprimer $\cos(nt)$ et $\sin(nt)$ en fonction de $\cos t$ et $\sin t$.

Linéarisation
Il s'agit d'écrire un produit $\cos^p t \sin^q t$, avec p et q dans $\mathbb{N}$, comme somme de termes de la forme $\cos(nt)$ ou $\sin(mt)$. On remplace cos et sin à l'aide des formules d'*Euler* :

$$\cos t = \frac{\mathrm{e}^{it} + \mathrm{e}^{-it}}{2}, \quad \sin t = \frac{\mathrm{e}^{it} - \mathrm{e}^{-it}}{2i}$$

Argument
Soit $z \neq 0$. Un argument de z est un réel t tel que : $z = |z|e^{it}$.
Si t_0 est un argument de z, l'ensemble des arguments de z est $\{t_0 + 2k\pi, k \in \mathbf{Z}\}$.
z a un unique argument dans $]-\pi, +\pi]$.
Si $z = |z|e^{it}$ et $z' = |z'|e^{it'}$, $zz' = |z||z'|e^{i(t+t')}$ ("l'argument d'un produit est la somme des arguments").
Si $z \neq 0$, et $n \in \mathbf{Z}$, $z^n = |z|^n e^{int}$.

Interprétation géométrique d'un nombre complexe, affixe
Dans un plan muni d'un repère orthonormé, on associe à $z = x + iy$ le point M de coordonnées (x, y) : on dira que le point M a pour affixe z. L'écriture $z = r\mathrm{e}^{i\theta}$ donne une autre représentation du point M d'affixe z, en *coordonnées polaires*. La correspondance entre coordonnées cartésiennes et coordonnées polaires est la suivante : le module r est égal à $r = \sqrt{x^2 + y^2}$; si $r \neq 0$, l'argument θ est déterminé à un multiple de 2π près par : $\cos\theta = x/r$ et $\sin\theta = y/r$.

Racines n$^{\text{ièmes}}$ d'un nombre complexe

Une des motivations fondamentales de l'introduction de $\mathbf{C}$ est la résolution d'équations algébriques. Ainsi, dans $\mathbf{C}$, l'équation $z^n = a$ où a est un paramètre complexe non nul et n un entier naturel, admet exactement n solutions, ce qui revient à dire que tout nombre complexe non nul possède exactement n racines $n^{\text{ièmes}}$ distinctes.
Soit $n \in \mathbb{N}^*$.
1) Racines $n^{\text{ièmes}}$ de l'unité :

$$\{z \in \mathbb{C}, z^n = 1\} = \{\omega_0, \omega_1, ..., \omega_{n-1}\}$$

où pour tout k dans $\{0, .., n-1\}$, $\omega_k = e^{2i\pi k/n}$.
2) Tout nombre complexe non nul $z = |z|e^{it}$, avec $t \in \mathbb{R}$, a exactement n racines $n^{\text{ièmes}}$ distinctes :

$$\{z' \in \mathbb{C}, z'^n = z\} = \{|z|^{1/n} e^{it/n} \omega_k, k \in \{0, .., n-1\}\}$$

Exemple : pour $n = 3$, les racines cubiques de l'unité sont $\{1, j, j^2\}$, avec $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = \mathrm{e}^{2i\pi/3}$. On a $\bar{j} = j^2$.

Droites et cercles

Soient A et B deux points distincts du plan d'affixes respectives a et b.
Un point M d'affixe z est sur la droite (AB) si et seulement si le rapport $\frac{z-a}{b-a}$ est réel.
L'ensemble des points M d'affixe z tel que $\arg(\frac{z-a}{z-b}) \equiv \theta \quad (2\pi)$, où θ est un réel fixé tel que $\sin\theta \neq 0$, est un arc de cercle passant par A et B. Si on remplace (2π) par (π), on obtient un cercle passant par A et B (dans les deux cas, il faut enlever B de l'ensemble obtenu).
L'équation du cercle de centre A et de rayon r s'écrit

$$|z - a| = r \ .$$

Similitudes

1) a et b étant deux nombres complexes donnés, $a \in \mathbf{C}^*$, l'application de $\mathbf{C}$ vers $\mathbf{C}$, $z \mapsto az + b$, s'interprète géométriquement comme une *similitude directe* du plan. Les cas particuliers sont :

$a = 1$: translation de vecteur d'affixe b

$|a| = 1,\ a \neq 1$: rotation d'angle l'argument de a
$a \in \mathbb{R} \setminus \{0, 1\}$: homothétie de rapport a.
2) a et b étant deux nombres complexes donnés, $a \in \mathbf{C}^*$, l'application de $\mathbf{C}$ vers $\mathbf{C}$, $z \mapsto a\overline{z} + b$, s'interprète géométriquement comme une *similitude indirecte* du plan. Les cas particuliers sont :
$|a| = 1$ et $a\bar{b} + b = 0$: symétrie orthogonale par rapport à une droite
$|a| = 1$ et $a\bar{b} + b \neq 0$: composée d'une symétrie orthogonale par rapport à une droite et d'une translation parallèle à cette droite.

Remarque : Structure de corps.

Soit E un ensemble muni de deux opérations notées + et .

On suppose que la loi + vérifie :
1) $\forall x \in E,\ \forall y \in E,\ x + y = y + x$ (+ est commutative)
2) $\forall x \in E, \forall y \in E, \forall z \in E,\ (x + y) + z = x + (y + z)$ (+ est associative)
3) Il existe un élément de E, noté en général 0, tel que :
$\forall x \in E, x + 0 = x$ (0 est élément neutre de +)
4) $\forall x \in E, \exists y \in E$ tel que $x + y = 0$. (Tout élément a un symétrique pour +)

On suppose que la loi . vérifie :
5) $\forall x \in E,\ \forall y \in E,\ x.y = y.x$ (. est commutative)
6) $\forall x \in E, \forall y \in E, \forall z \in E,\ (x.y).z = x.(y.z)$ (. est associative)
7) Il existe un élément de E, noté en général 1, tel que :
$\forall x \in E, x.1 = x$ (1 est élément neutre de .)
8) $1 \neq 0$, et $\forall x \in E \setminus \{0\}, \exists y \in E$ tel que $x.y = 1$. (Tout élément non nul a un symétrique pour .)

On suppose enfin que . est distributive par rapport à + :
9) $\forall x \in E, \forall y \in E, \forall z \in E,\ x.(y + z) = x.y + x.z$

On dit alors que $(E, +, .)$, ou plus simplement E s'il n'y a pas ambiguïté, est un corps commutatif.

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps commutatifs.
$\mathbf{Z}$ ne vérifie pas 8), mais vérifie toutes les autres propriétés : on dit que $\mathbf{Z}$ est un anneau commutatif.
Un ensemble muni d'une loi qui vérifie 1),2),3) et 4) est appelé groupe commutatif.

CHAPITRE 3

POLYNOMES

I. DEFINITION

On fixe $K = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.
Un polynôme à coefficients dans K est une suite $(a_i)_{i\in\mathbb{N}}$ d'éléments de K qui est presque nulle, c'est-à-dire telle qu'il existe un entier $n \in \mathbb{N}$ vérifiant : $a_i = 0$ pour tout $i > n$.
Pour tout i de $\mathbb{N}$, a_i s'appelle le coefficient de degré i du polynôme.

Somme et multiplication par un élément de K
Si $P = (a_i)_{i\in\mathbb{N}}$, $Q = (b_i)_{i\in\mathbb{N}}$ sont des polynômes et $\lambda \in K$, on définit les polynômes $P + Q = (a_i + b_i)_{i\in\mathbb{N}}$, $P - Q = (a_i - b_i)_{i\in\mathbb{N}}$, et $\lambda.P = \lambda P = (\lambda a_i)_{i\in N}$.

Pour $i \in \mathbb{N}$, on note X^i le polynôme dont tous les coefficients sont nuls sauf le coefficient de degré i qui vaut 1. On note 0 le polynôme dont tous les coefficients sont nuls, on note 1 le polynôme X^0.

Soit $P = (a_i)_{i\in\mathbb{N}}$ un polynôme, et n dans $\mathbb{N}$ tel que $a_i = 0\ \forall i > n$. Alors

$$P = a_0 + a_1X + ... + a_nX^n = \sum_{i=0}^{n} a_iX^i$$

P se note aussi $P(X)$.
L'ensemble des polynômes à coefficients dans K se note $K[X]$.

On a : $P + Q = Q + P$, $(P + Q) + R = P + (Q + R)$, $P + 0 = P$, $P + (-P) = 0$, $(\lambda + \mu).P = \lambda.P + \mu.P$, $\lambda.(P + Q) = \lambda.P + \lambda.Q$, $\lambda.(\mu.P) = (\lambda\mu).P$ pour tous polynômes P, Q et R, et éléments λ et μ dans K.

Produit de polynômes
Si $P = (a_i)_{i\in\mathbb{N}}$ et $Q = (b_i)_{i\in\mathbb{N}}$ sont des polynômes, on définit le polynôme produit

$PQ = (c_i)_{i\in\mathbb{N}}$ par : pour tout i de $\mathbb{N}$,

$$c_i = a_0b_i + ... + a_kb_{i-k} + ... + a_ib_0 = \sum_{(k,l)\in\mathbb{N}^2 \text{ t.q. } k+l=i} a_kb_l = \sum_{k=0}^{i} a_kb_{i-k} = \sum_{l=0}^{i} a_{i-l}b_l$$

On a alors : $PQ = QP$, $(PQ)R = P(QR)$, $1.P = P$, $P(Q+R) = PQ + PR$ pour tous polynômes P, Q et R.

On définit $P^0 = 1$, $P^1 = P$, $P^2 = P\,P$, $P^3 = P\,P\,P$, $P^n = P...P$ (n polynômes P) pour n dans $\mathbb{N}$. On a bien $X^n = X...X$ (n fois).

Formule du binôme de Newton
Soient P et Q dans $K[X]$, et $n \in \mathbb{N}$:

$$(P+Q)^n = \sum_{k=0}^{n} C_n^k P^k Q^{n-k}$$

où pour k dans $\mathbb{N}$ tel que $k \leq n$, $C_n^k = \dfrac{n!}{k!(n-k)!} \in \mathbb{N}$

Divisibilité
Pour A et B dans $K[X]$, on dit que B divise A s'il existe un polynôme Q dans $K[X]$ tel que $A = BQ$. On note $B|A$.

II. DEGRE ET DIVISION EUCLIDIENNE

Degré
Soit $P = (a_i)_{i\in\mathbb{N}}$ un polynôme non nul. Le plus grand entier n tel que $a_n \neq 0$ est appelé le degré de P, et se note $\deg(P)$.
Si $P = 0$, on pose $\deg(P) = -\infty$.
On utilisera les règles : $(-\infty) + (-\infty) = -\infty$, $n + (-\infty) = -\infty$, $-\infty \leq n$ et $n \not\leq -\infty$ pour tout n dans $\mathbb{N}$.

Pour tous polynômes P et Q,

$$\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\} \text{ et } \deg(PQ) = \deg(P) + \deg(Q)$$

Si $\deg P \neq \deg Q$, alors $\deg(P+Q) = \max\{\deg(P), \deg(Q)\}$.

Soient P, Q et R des polynômes.

Si $PQ = PR$ et $P \neq 0$, alors $Q = R$.

Si $PQ = 0$, alors $P = 0$ ou $Q = 0$.

Division Euclidienne

Soient A et B deux polynômes de $K[X]$, avec $B \neq 0$. Il existe un unique couple (Q, R) dans $K[X] \times K[X]$ tel que :

$$A = BQ + R, \text{ et } \deg(R) < \deg(B)$$

Q s'appelle le quotient de la division euclidienne de A par B, R s'appelle le reste de la division euclidienne de A par B.

III. DERIVEES

Fonction polynôme

Soit $P = a_0 + a_1X + ... + a_nX^n$ un polynôme de $K[X]$. La fonction polynôme associée à P est l'application f_P de K dans K qui à tout x de K associe $P(x) = a_0 + a_1x + ... + a_nx^n$.

$f_P = f_Q$ si et seulement si $P = Q$. On peut donc définir un polynôme par sa fonction polynôme.

Composition de polynômes

Si P et Q sont deux polynômes, on définit le polynôme $P \circ Q$ par $P \circ Q(x) = P(Q(x))$ pour tout x de K.

Dérivée

Soit $P = \sum_{i=0}^{n} a_iX^i$ un polynôme de $K[X]$. Le polynôme dérivé de P se note P', et vaut $P' = \sum_{i=1}^{n} ia_iX^{i-1}$. "On dérive un polynôme comme la fonction polynôme associée".

Pour P et Q dans $K[X]$, $(PQ)' = P'Q + Q'P$. Si $\deg(P) \geq 1$, $\deg(P') = \deg(P) - 1$. Si $\deg(P) \leq 0$, $P' = 0$.

On définit par récurrence les dérivées successives d'un polynôme P. $P^{(0)} = P$, $P^{(1)} = P'$, $P^{(2)} = (P')'$ (aussi noté P"), et pour tout k de $\mathbb{N}$, $P^{(k+1)} = (P^{(k)})'$. $P^{(k)}$ est le polynôme P dérivé k fois.

Si P est un polynôme de degré $n \in \mathbb{N}$, alors $P^{(n)}$ est un polynôme constant non nul, et $P^{(k)} = 0$ pour tout $k > n$.

Attention à ne pas confondre, $P^2 = PP$, $P \circ P$ et $P^{(2)} = P$".

Formule de Taylor pour les polynômes
Soit $P \in K[X]$ un polynôme de degré n, et $a \in K$. Alors

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

$$= P(a)+(X-a)P'(a)+\frac{(X-a)^2}{2}P"(a)+...+\frac{(X-a)^k}{k!}P^{(k)}(a)+...+\frac{(X-a)^n}{n!}P^{(n)}(a)$$

On a aussi $P(X+a) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}X^k$, et $P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!}X^k$.

Si $P = (a_i)_{i \in \mathbb{N}}$ est un polynôme, alors pour tout i de $\mathbb{N}$:

$$a_i = \frac{P^{(i)}(0)}{i!}$$

IV. RACINES

On fixe $P \in K[X]$.
Un élément a de K est une racine (ou un zéro) de P si $P(a) = 0$.
a est racine de P ssi $X - a | P$ ("On peut mettre $X - a$ en facteur dans P").

Théorème :
Pour a dans K et $m \in \mathbb{N}^*$,

$$P(a) = P'(a) = ... = P^{(m-1)}(a) = 0 \Longleftrightarrow (X-a)^m | P$$

Racines multiples
Soit m dans $\mathbb{N}^*$.

a dans K est racine d'ordre (de multiplicité) m de P si $P^{(k)}(a) = 0$ pour $k \in \{0, ..., m-1\}$, et $P^{(m)}(a) \neq 0$.
Si $m = 1$, on dit que a est racine simple de P. Si $m = 2$, a est racine double de P.

a est racine d'ordre m de $P \iff (X-a)^m$ divise P et $(X-a)^{m+1}$ ne divise pas P

Si $l \geq 1$, $r_1, ..., r_l$ sont des racines distinctes de P d'ordre de multiplicité respectives m_1, ..., m_l, alors il existe Q dans $K[X]$, tel que :

$$P = (X - r_1)^{m_1}(X - r_2)^{m_2}...(X - r_l)^{m_l}Q$$

Nombre de racines et degré
Si $P \neq 0$, toute racine a de P a un ordre de multiplicité m_a dans $\mathbb{N}^*$. Compter les racines avec leur ordre de multiplicité signifie compter chaque racine a m_a fois.

Un polynôme non nul de degré n a au plus n racines, comptées avec leur ordre de multiplicité.
En particulier, un polynôme non nul a un nombre fini de racines.

V. RACINES DANS $\mathbf{C}[\mathbf{X}]$

Théorème de D'alembert-Gauss
Dans $\mathbb{C}[X]$, tout polynôme non nul de degré n a exactement n racines comptées avec leur ordre de multiplicité. (dem HP)

Factorisation dans $\mathbf{C}[X]$
Soit $P = a_0 + a_1X + ... + a_nX^n$ un polynômes à coefficients complexes de degré $n \geq 1$. Il existe $l \geq 1$, $r_1, ..., r_l$ des complexes distincts, $m_1, ..., m_l$ des entiers ≥ 1, $\lambda \in \mathbb{C}^*$ tels que :

$$P = \lambda(X - r_1)^{m_1}...(X - r_l)^{m_l}$$

l, λ et l'ensemble $\{(r_1, m_1), ..., (r_l, m_l)\}$ sont uniques. $r_1, ..., r_l$ sont les racines de P, m_1,...,m_l sont leurs ordres de multiplicité respectifs. On a aussi $\lambda = a_n$ et $m_1 + ... + m_l = n$.

La somme des racines, comptées avec leur ordre de multiplicité, est $r_1 m_1 + ... + r_l m_l = -a_{n-1}/a_n$.
Le produit des racines, comptées avec leur ordre de multiplicité, est $r_1^{m_1}...r_l^{m_l} = (-1)^n a_0/a_n$.

VI. RACINES DANS $\mathbb{R}[X]$

Soit P un polynôme à coefficients réels. Si on se place dans $\mathbb{R}[X]$, les racines de P sont par définition réelles. Mais P peut également être vu comme un polynôme de $\mathbb{C}[X]$.
Pour tout z de $\mathbb{C}$, $P(\bar{z}) = \overline{P(z)}$. Donc si $\alpha \in \mathbb{C}$ est une racine de P en tant que polynôme de $\mathbb{C}[X]$, $\bar{\alpha}$ l'est également. De même si $\alpha \in \mathbb{C}$ est une racine d'ordre $m \geq 1$ de P en tant que polynôme de $\mathbb{C}[X]$, $\bar{\alpha}$ l'est également.

En regroupant toute racine complexe non réelle avec son conjugué, on peut factoriser P dans $\mathbb{R}[X]$.

Factorisation dans $\mathbb{R}[X]$
Soit P un polynômes à coefficients réels de degré $n \geq 0$. Il existe λ dans $\mathbb{R}^*$, l et h dans $\mathbb{N}$, $r_1, ..., r_l$ des réels distincts, $m_1, ..., m_l$ des entiers ≥ 1, $(b_1, c_1), ..., (b_h, c_h)$ des couples distincts de réels, $d_1, ..., d_h$ des entiers ≥ 1 tels que :

$$P = \lambda(X - r_1)^{m_1}...(X - r_l)^{m_l}(X^2 + b_1 X + c_1)^{d_1}...(X^2 + b_h X + c_h)^{d_h}$$

avec : pour $i = 1, ..., h$, $b_i^2 - 4c_i < 0$, λ est le coefficient de plus haut degré de P, $r_1 + ... + r_l + 2d_1 + ... + 2d_h = n$.
Cette écriture est unique, à l'ordre près. r_1, r_l sont les racines de P dans $\mathbb{R}$, et m_1,...,m_l sont leurs ordres de multiplicité respectifs.

Il s'ensuit que tout polynôme à coefficients réels de degré impair a au moins une racine réelle.

CHAPITRE 4

SYSTEMES LINEAIRES

K est $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.
Résoudre un système linéaire de n équations à p inconnues $x_1, x_2, \ldots, x_p$, c'est déterminer tous les p-uplets $(x_1, \ldots, x_p)$ de K^p vérifiant n relations linéaires :

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1p}x_p & = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2p}x_p & = b_2 \\ \qquad\qquad \vdots \quad \vdots & \qquad\quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{np}x_p & = b_n \end{cases}$$

où les coefficients a_{ij} ,b_i sont des éléments de K fixés. Les b_i s'appellent les seconds membres des équations.
Tout p-uplet vérifiant les équations s'appelle une solution du système.

Résultats généraux
Lorsque les seconds membres sont nuls ($b_i = 0$ pour tout $i \in \{1, .., n\}$), le système est dit homogène ; $(0, \ldots, 0)$ est toujours solution.
Dans le cas où les b_i ne sont pas tous nuls, l'ensemble des solutions du système peut être vide, on dit alors que le système est incompatible.

Opérations sur un système
Deux systèmes sont équivalents s'ils ont le même ensemble de solutions. La technique de résolution d'un système consiste, par une suite d'opérations sur les lignes du système, à remplacer le système initial par un système équivalent plus simple. L'idée est de faire intervenir le moins d'inconnues possibles dans chaque ligne.
Les opérations qui remplacent un système par un système équivalent sont :

a) Multiplier une ligne par un scalaire non nul.
b) Ajouter à une ligne, une autre ou plusieurs autres lignes.
c) Echanger deux lignes.

Méthode du pivot
Considérons deux lignes d'un système linéaire :
$L_1 : \quad a_{11}x_1 + a_{12}x_2 + \cdots a_{1p}x_p = b_1$
$L_2 : \quad a_{21}x_1 + a_{22}x_2 + \cdots a_{2p}x_p = b_2$

Si $a_{11} \neq 0$ alors en remplaçant L_2 par $L_2 - \frac{a_{21}}{a_{11}} L_1$, on obtient un système équivalent composé d'une nouvelle ligne L'_2 où ne figure plus l'inconnue x_1 :
$L'_2 : (a_{22} - \frac{a_{21}}{a_{11}} a_{12})x_2 + \cdots (a_{2p} - \frac{a_{21}}{a_{11}} a_{1p})x_p = b_2 - \frac{a_{21}}{a_{11}} b_1$
En répétant cette opération pour les autres lignes du système, on obtient un système équivalent au système initial composé de la ligne L_1 inchangé, et de nouvelles lignes $L'_2, \ldots, L'_n$ où x_1 ne figure plus.
Le rôle du coefficient a_1, non nul, est primordial : on dit que a_1 est le pivot de cette suite d'opérations.
Puis, on peut considérer $L'_2, \ldots, L'_n$ comme un sous-système du système initial, dont les inconnues sont $x_2, \ldots, x_p$. On cherche un pivot non nul pour pouvoir procéder comme précédemment.
Au bout d'un nombre fini d'opérations, on aboutit à une incompatibilité ou bien à un système équivalent de la forme :

$$\begin{cases} a'_{11}x_1 + a'_{12}x_2 + a'_{13}x_3 + \cdots a'_{1p}x_p &= b'_1 \\ \qquad a'_{22}x_2 + a'_{23}x_3 + \cdots a'_{2p}x_p &= b'_2 \\ \vdots \qquad\qquad\qquad\qquad \vdots &= \vdots \\ \qquad\qquad a'_{rr}x_r + \cdots + a'_{rp}x_p &= b'_r \end{cases}$$

où $r \leq n$. En effet certaines lignes peuvent disparaitre : $0 = 0$ ou deux lignes identiques...
Les pivots successifs apparaissent en tête de chaque ligne : $a'_{11}, a'_{22}, \ldots a'_{rr}$, on suppose donc ces termes non nuls.
On peut également être amené à échanger la place des inconnues dans les lignes.
Le système final est ainsi constitué de r équations d'inconnues $x'_1, \ldots, x'_r, \ldots, x'_p$ où les x'_i sont les x_i à l'ordre près.
On achève la résolution en exprimant, à partir de la dernière ligne, x'_r en fonction de $x'_{r+1}, \ldots, x'_p$, puis par récurrence, en remontant ligne par ligne, on détermine $x'_{r-1}, \ldots, x'_1$ en fonction de $x'_{r+1}, \ldots, x'_p$.

Rang

Si on appelle $\mathcal{S}$ le système initial de n équations à p inconnues, on peut lui associer le système homogène $\mathcal{S}_0$ obtenu, à partir de $\mathcal{S}$, en remplaçant tous les seconds membres par 0.
En opérant sur $\mathcal{S}_0$ par la méthode du pivot, on obtient un système équivalent de r équations. Cet entier r est indépendant de la façon dont on opère : on l'appelle le rang du système $\mathcal{S}$.
Le rang n'indique pas, en général, si le système $\mathcal{S}$ est compatible.
D'autre part, le rang est toujours inférieur (ou égal) au nombre d'équations du système initial, ainsi qu'au nombre d'inconnues.

Résultats généraux

En reprenant les notations précédentes, on peut donner la structure de l'ensemble des solutions de $\mathcal{S}$ ou de $\mathcal{S}_0$ (voir le cours d'algèbre 2 pour la notion de "sous-espace vectoriel").
L'ensemble des solutions de $\mathcal{S}_0$ est un sous-espace vectoriel de K^p de dimension $p-r$, que l'on appellera A.
L'ensemble des solutions de $\mathcal{S}$ est soit :
- vide, dans ce cas $\mathcal{S}$ est un système incompatible.
- soit de la forme $X^S + A$.

où $X^S = (x_1^S, x_2^S, \cdots x_p^S)$ est une solution particulière de $\mathcal{S}$.
Cette dernière propriété se mémorise ainsi :
Solution générale de $\mathcal{S}$ = solution particulière de $\mathcal{S}$ + solution générale de $\mathcal{S}_0$.

Cas particuliers
Si $r = p$, $A = \{(0, \ldots, 0)\}$ et $\mathcal{S}$ admet au plus une solution.
Si $r = n$, $\mathcal{S}$ est toujours compatible.
Si $p = n = r$, $\mathcal{S}$ est appelé système de Cramer, il admet une unique solution.

Mise en œuvre numérique
On suppose ici que $\mathcal{S}$ est un système de Cramer, de n équations à n inconnues.
Lorsqu'on résout à la main un système, on opère à l'aide des pivots les plus commodes : 1 ou -1 par exemple.
Mais, lorsque l'on programme la méthode sur ordinateur, on choisit, pour chaque inconnue, les pivots les plus grands (en valeur absolue), car on démontre que l'on minimise ainsi les erreurs de calculs produites par la machine.
Si l'on s'astreint à ne pas modifier l'ordre des inconnues, c'est la méthode du pivot partiel, on aboutit à :

$$\begin{cases} a'_{11}x_1 + a'_{12}x_2 + \cdots + a'_{1n}x_n &= b'_1 \\ \quad a'_{21}x'_2 + \cdots + a'_{2n}x_n &= b'_2 \\ \quad\vdots \quad\vdots \qquad\qquad\qquad &\vdots \\ \qquad\qquad\qquad\qquad a'_{nn}x_n &= b'_n \end{cases}$$

le système est dit triangulaire.

Puis dans la phase dite de remontée, on calcule successivement $x_n, x_{n-1}, \ldots, x_1$.

CHAPITRE 5

MATRICES

1 Introduction

Rappelons qu'un système linéaire de n équations à p inconnues est de la forme

$$(S) \qquad \left\{ \begin{array}{rcl} a_{11}x_1 + \ldots + a_{1j}x_j + \ldots + a_{1p}x_p & = & b_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots & & \ldots \\ a_{i1}x_1 + \ldots + a_{ij}x_j + \ldots + a_{ip}x_p & = & b_i \\ \ldots\ldots\ldots\ldots\ldots\ldots & & \ldots \\ a_{n1}x_1 + \ldots + a_{nj}x_j + \ldots + a_{np}x_p & = & b_n \end{array} \right.$$

L'objet de ce chapitre est d'introduire un système de notations afin d'alléger la formule précédente : nous allons ramener l'écriture du système linéaire (S) à l'égalité :

$$AX = b$$

où A, X et b seront des tableaux de nombres, appelés matrices. Ici

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1j} & \ldots & a_{1p} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{i1} & \ldots & a_{ij} & \ldots & a_{ip} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nj} & \ldots & a_{np} \end{pmatrix} \quad , \quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_j \\ \vdots \\ x_p \end{pmatrix} \quad \text{et} \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_j \\ \vdots \\ b_n \end{pmatrix}$$

Nous définirons ce que signifie le produit AX, et l'égalité $AX = b$.

Lorsque $n = p$, et pour certaines matrices A particulières (appelées matrices inversibles), la solution du système (S) sera unique, et donnée par la formule

$$X = A^{-1}b$$

où A^{-1} sera la matrice inverse de A que l'on apprendra à calculer grâce à l'algorithme de Gauss-Jordan.

2 Définitions

2.1 Définitions et notations

Définition 2.1 (Matrices)
Soient n et p deux entiers positifs non nuls. On appelle matrice à coefficients réels (resp. complexes) la donnée de $n \times p$ nombres réels (resp. complexes) notés

$$(a_{ij})_{i\in\{1,\dots,n\},\ j\in\{1,\dots,p\}}$$

On représente la matrice sous forme d'un tableau A à n lignes et p colonnes :

$$A = \begin{pmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1p} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} & \dots & a_{ij} & \dots & a_{ip} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nj} & \dots & a_{np} \end{pmatrix}$$

On dit que a_{ij} est le *terme général de la matrice A* : le premier indice (ici i) désigne toujours *l'indice de ligne* et le second indice (ici j) *l'indice de colonne*. On écrit aussi sous forme condensée : $A = (a_{ij})_{n,p}$ ou encore $A = (a_{ij})$ s'il n'y a aucune ambiguïté.

Le couple (n, p) s'appelle *le format de la matrice*.

Définition 2.2 (Egalité de deux matrices)
Deux matrices $A = (a_{ij})_{n,p}$ et $B = (b_{ij})_{m,q}$ sont égales si et seulement si :
- A et B ont même format : $n = m$ et $p = q$
et
- $\forall i \in \{1,\dots,n\},\ \forall j \in \{1,\dots,p\},\quad a_{ij} = b_{ij}$.

On désigne par $M_{n,p}(\mathbb{R})$ (resp. $M_{n,p}(C)$) l'ensemble des matrices à coefficients réels (resp. complexes) à n lignes et p colonnes. Dans la suite du chapitre, pour simplifier l'exposé, on étudie les matrices à coefficients réels, mais les définitions et les propriétés restent vraies pour les matrices à coefficients complexes. On écrira donc simplement $M_{n,p}$ au lieu de $M_{n,p}(\mathbb{R})$ ou $M_{n,p}(C)$.

2.2 Matrices particulières

- *la matrice nulle* dans $M_{n,p}$: on la note O, c'est la matrice à n lignes et p colonnes dont tous les coefficients valent 0.
- *les matrices élémentaires* dans $M_{n,p}$: on les note E^{ij} (i et j fixés, $1 \le i \le n$, $1 \le j \le p$). La matrice E^{ij} est la matrice dont tous les coefficients sont nuls, sauf celui qui se trouve dans la ligne i et la colonne j, et qui vaut 1.

- *matrice ligne :* c'est une matrice de format $(1, p)$.
- *matrice colonne :* c'est une matrice de format $(n, 1)$.
- *matrice carrée d'ordre n :* c'est une matrice de format (n, n). L'ensemble des matrices carrées d'ordre n est noté $M_n(\mathbb{R})$ pour les matrices à coefficients réels, $M_n(C)$ pour les matrices à coefficients complexes. Si $n = 1$, on identifie $M_1(\mathbb{R})$ et $\mathbb{R}$.

3 Opérations sur les matrices

3.1 Somme de deux matrices de $M_{n,p}$

Définition 3.1 *Soient $A = (a_{ij})$ et $B = (b_{ij})$ deux éléments de $M_{n,p}$. On appelle somme de A et B la matrice $C = (c_{ij})$ de format (n, p) dont le terme général est :*

$$\forall i \in \{1, \ldots, n\},\ \forall j \in \{1, \ldots, p\},\ \ c_{ij} = a_{ij} + b_{ij}$$

On note $C = A + B$.

Attention : on ne peut additionner que des matrices de même format.

Proposition 3.2 (Propriétés de l'addition)

1. *elle est commutative :*

$$\forall A \in M_{n,p},\ \forall B \in M_{n,p}, \qquad A + B = B + A.$$

2. *elle est associative :*

$$\forall A \in M_{n,p},\ \forall B \in M_{n,p},\ \forall C \in M_{n,p}, \qquad A+(B+C) = (A+B)+C\ .$$

3. *elle admet un élément neutre, qui est la matrice nulle :*

$$\forall A \in M_{n,p}, \qquad A + O = O + A = A\ .$$

4. *toute matrice A a un unique symétrique pour l'addition, noté $-A$:*

$$\forall A \in M_{n,p},\ \ A + (-A) = (-A) + A = O,\ \ \text{avec} - A = (-a_{ij})\ \ \text{si}\ \ A = (a_{ij})$$

Remarque : Grâce à la propriété d'associativité, on écrira désormais $A+B+C$ pour $A + (B + C) = (A + B) + C$.

Démonstration :

1. Si $A = (a_{ij})$ et $B = (b_{ij})$, le terme général de la matrice $A + B$ est $(a_{ij} + b_{ij})$, tandis que le terme général de la matrice $B+A$ est $(b_{ij}+a_{ij})$. Comme $(a_{ij}+b_{ij}) = (b_{ij} + a_{ij})$, on en déduit que les deux matrices $A + B$ et $B + A$, qui ont même format (n, p) et même terme général, sont égales.

2. Si $A = (a_{ij})$, $B = (b_{ij})$ et $C = (c_{ij})$, la matrice $B + C$ a pour terme général $(b_{ij} + c_{ij})$ et la matrice $A + (B + C)$ a pour terme général $a_{ij} + (b_{ij} + c_{ij})$. De même, la matrice $(A + B) + C$ a pour terme général $(a_{ij} + b_{ij}) + c_{ij}$. Comme $a_{ij} + (b_{ij} + c_{ij}) = (a_{ij} + b_{ij}) + c_{ij}$, les matrices $A + (B + C)$ et $(A + B) + C$, qui ont même format (n, p) et même terme général sont égales.

3. Si $A = (a_{ij})$, comme la matrice O a pour terme général 0, la matrice $A + O$ a pour terme général $a_{ij} + 0 = a_{ij}$. Donc les matrices A et $A + O$, qui ont même format (n, p) et même terme général, sont égales. On vérifie de même l'égalité $O + A = A$.

4. Si $A = (a_{ij})$, alors la somme $A + (-A)$ a pour terme général $(a_{ij} + (-a_{ij})) = 0$. Comme les matrices $A + (-A)$ et O ont même format (n, p) et même terme général, elles sont égales.

   Réciproquement, si $B = (b_{ij})$ est un symètrique de A, alors on doit avoir $A+B = O$, c'est-à-dire $a_{ij} + b_{ij} = 0$ pour tout $i \in 1, \ldots, n$ et tout $j \in 1, \ldots, p$. Donc on a $b_{ij} = -a_{ij}$ pour tout $i \in 1, \ldots, n$ et tout $j \in 1, \ldots, p$. Par conséquent, toute matrice a un unique symétrique.

□

3.2 Multiplication d'une matrice de $M_{n,p}$ par un scalaire

Définition 3.3 *Soit $A = (a_{ij})$ une matrice de $M_{n,p}$, et soit λ un scalaire (réel ou complexe suivant le cas). On appelle multiplication de la matrice A par le scalaire λ la matrice $B = (b_{ij})$ de format (n, p) dont le terme général est*

$$\forall i \in \{1, \ldots, n\},\ \forall j \in \{1, \ldots, p\}, \qquad b_{ij} = \lambda a_{ij} \ .$$

On note $B = \lambda A$.

Proposition 3.4 (Propriétés de la multiplication par un scalaire)
$\forall A \in M_{n,p}$, $\forall B \in M_{n,p}$, $\forall (\lambda, \mu) \in \mathbb{R} \times \mathbb{R}$,

1. $\lambda(A + B) = \lambda A + \lambda B$
2. $(\lambda + \mu)A = \lambda A + \mu A$
3. $\lambda(\mu A) = (\lambda\mu)A = \mu(\lambda A)$
4. $1.A = A$

Preuve : On pose $A = (a_{ij})$ et $B = (b_{ij})$.

1. La matrice $(A+B)$ a pour terme général $(a_{ij}+b_{ij})$, et la matrice $\lambda(A+B)$ a pour terme général $(\lambda(a_{ij}+b_{ij}))$. D'autre part, les matrices λA et λB ont pour terme général respectivement (λa_{ij}) et (λb_{ij}). Donc la matrice $\lambda A + \lambda B$ a pour terme général $(\lambda a_{ij}) + (\lambda b_{ij})$. Comme $\lambda(a_{ij} + b_{ij}) = (\lambda a_{ij}) + (\lambda b_{ij})$, on en déduit que les matrices $\lambda(A + B)$ et $\lambda A + \lambda B$, qui ont même format (n, p) et même terme général, sont égales.

2. La matrice $(\lambda+\mu)A$ a pour terme général $((\lambda+\mu)a_{ij})$. D'autre part, les matrices λA et μA ont pour terme général respectivement (λa_{ij}) et (μa_{ij}). Donc la matrice $\lambda A+\mu A$ a pour terme général $(\lambda a_{ij})+(\mu a_{ij})$. Comme $(\lambda+\mu)a_{ij} = (\lambda a_{ij})+(\mu a_{ij})$, on en déduit que les matrices $(\lambda + \mu)A$ et $\lambda A + \mu A$, qui ont même format (n, p) et même terme général, sont égales.

3. La matrice μA a pour terme général (μa_{ij}), et la matrice $\lambda(\mu A)$ a alors pour terme général $(\lambda(\mu a_{ij}))$. D'autre part, la matrice $(\lambda\mu)A$ a pour terme général $(\lambda\mu a_{ij})$. Comme $(\lambda(\mu a_{ij})) = (\lambda\mu a_{ij})$, on en déduit que les matrices $\lambda(\mu A)$ et $(\lambda\mu)A$, qui ont même format (n, p) et même terme général, sont égales.

   L'égalité $(\lambda\mu)A = \mu(\lambda A)$ s'obtient de la même façon.

4. La matrice $1.A$ a pour terme général $1a_{ij} = a_{ij}$. Donc les matrices $1A$ et A, qui ont même format (n, p) et même terme général, sont égales.

□

Théorème 3.5 *Toute matrice $A = (a_{ij})$ de $M_{n,p}$ vérifie :*

$$A \;=\; \sum_{i\in\{1,\ldots,n\},\; j\in\{1,\ldots,p\}} a_{ij}E^{ij}$$

Preuve : Soit $A = (a_{ij})$ un élément de $M_{n,p}$. On affirme que

$$\sum_{i\in\{1,\ldots,n\},\; j\in\{1,\ldots,p\}} a_{ij}E^{ij} \;=\; A$$

En effet, comme les deux matrices ont même format, il suffit de montrer qu'elles ont même terme général. Le terme général de la matrice

$$\sum_{i\in\{1,\ldots,n\},\; j\in\{1,\ldots,p\}} a_{ij}E^{ij}$$

est

$$\left(\sum_{i\in\{1,\ldots,n\},\; j\in\{1,\ldots,p\}} a_{ij}e^{ij}_{kl}\right)_{k,l},$$

c'est-à-dire a_{kl}. Il y a bien égalité entre les deux matrices.

□

3.3 Produit de deux matrices

Définition 3.6 *Soient $A = (a_{ij})_{n,p}$ un élément de $M_{n,p}$ et $B = (b_{ij})_{p,q}$ un élément de $M_{p,q}$. On appelle produit de A par B la matrice C de format (n, q) dont le terme général c_{ij} est défini par :*

$$\forall i \in \{1, \ldots, n\},\ \forall j \in \{1, \ldots, q\}\ , \qquad c_{ij} = \sum_{k=1}^{p} a_{ik} b_{kj}$$

On note $C = AB$.

Attention : Le produit de deux matrices n'est pas toujours défini. Le produit AB n'a de sens que si le nombre de colonnes de A est égal au nombre de lignes de B.

Pour éviter les erreurs , il est conseillé d'adopter la présentation suivante des calculs, proposée ici sur un exemple :

$$B = \begin{pmatrix} 2 & 1 & 0 & 1 \\ 0 & 1 & 0 & 3 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \end{pmatrix} \qquad AB = \begin{pmatrix} 5 & 3 & 3 & 10 \\ 2 & 1 & 2 & 5 \end{pmatrix}$$

Cette disposition permet de vérifier que la matrice AB obtenue a le même nombre de lignes que A et le même nombre de colonnes que B ; elle a de plus l'avantage de bien se prêter aux calculs itérés.

Proposition 3.7 (Propriétés du produit matriciel)
Avec les hypothèses convenables pour que les produits existent :

1. *le produit matriciel est associatif :*

$$A(BC) = (AB)C$$

2. *il est distributif par rapport à l'addition :*

$$A(B + C) = AB + AC \qquad \text{et} \qquad (A + B)C = AC + BC$$

3. $\forall \lambda \in \mathbb{R}$,

$$A(\lambda B) = (\lambda A)B = \lambda(AB)$$

Remarque : On note désormais ABC le produit $A(BC) = (AB)C$.

Ces propriétés sont des propriétés "agréables" qui correspondent bien aux calculs auxquels jusqu'à présent vous êtes habitués.

Mais attention ! Ce produit matriciel recèle aussi quelques pièges :

- **Le produit matriciel n'est pas commutatif :**

  - le produit AB peut avoir un sens alors que BA n'en a pas : c'est le cas lorsque A est une matrice (n, p) et B une matrice (p, q) avec $n \neq q$.

  - même si les produits AB et BA ont un sens, les matrices AB et BA ne sont en général pas du même format, donc certainement pas égales ; par exemple si A est une matrice $(3, 2)$ et B une matrice $(2, 3)$, alors AB est une matrice $(3, 3)$ et BA une matrice $(2, 2)$.

  - enfin même dans le cas a priori le plus favorable, c'est-à-dire si A et B sont des matrices carrées de même ordre n, les deux matrices AB et BA sont aussi des matrices carrées de même ordre n, mais en général elles ne sont pas égales.

- **On peut avoir $AB = O$, sans que $A = O$ ou $B = O$.**

  Une conséquence de cette propriété est qu'on n'a pas le droit de simplifier une égalité matricielle : $AB = AC$ n'implique pas forcément $B = C$.

Démonstration de la proposition 3.7 :

1. Si $A = (a_{ij})_{n,p}$, $B = (b_{ij})_{p,q}$, $C = (c_{ij})_{q,r}$, alors :
   La matrice $D = BC$ a pour terme général $D = (d_{lj})_{pr}$ où

$$d_{lj} = \sum_{k=1}^{q} b_{lk} c_{kj}$$

   et la matrice $E = A(BC) = AD$ a alors pour terme général $E = (e_{ij})_{n,r}$ où

$$e_{ij} = \sum_{l=1}^{p} a_{il} d_{lj} = \sum_{l=1}^{p} \sum_{k=1}^{q} a_{il} b_{lk} c_{kj}$$

   D'autre part, la matrice $F = (AB)$ a pour terme général $F = (f_{ik})_{n,q}$ où

$$f_{ik} = \sum_{l=1}^{p} a_{il} b_{lk}$$

   et la matrice $G = (AB)C = FC$ a pour terme général $G = (g_{ij})_{n,r}$ où

$$g_{ij} = \sum_{k=1}^{q} f_{ik} c_{kj} = \sum_{k=1}^{q} \sum_{l=1}^{p} a_{il} b_{lk} c_{kj}$$

Comme on peut permuter deux sommes finies, on en déduit que les matrices $E = A(BC)$ et $G = (AB)C$, qui ont même format (n, r) et même terme général, sont égales.

2. Montrons l'égalité $A(B + C) = AB + AC$. Si $A = (a_{ij})_{n,p}$, $B = (b_{ij})_{p,q}$, $C = (c_{ij})_{p,q}$, alors la matrice $(B + C)$ a pour terme général $(b_{ij} + c_{ij})$ et pour format (p, q). Le produit $D = A(B+C)$ a alors pour format (n, q) et pour terme général

$$d_{ij} = \sum_{k=1}^{p} a_{ik}(b_{kj} + c_{kj}) \ .$$

D'autre part, les matrices AB et AC ont même format (n, q) et pour terme général respectif $(\sum_{k=1}^{p} a_{ik}b_{kj})$ et $(\sum_{k=1}^{p} a_{ik}c_{kj})$. Donc la matrice $E = AB + AC$ a pour format (n, q) et pour terme général

$$e_{ij} = \sum_{k=1}^{p} a_{ik}b_{kj} + \sum_{k=1}^{p} a_{ik}b_{kj} = d_{ij}$$

Comme les matrices D et E ont même format (n, q) et même terme général $d_{ij} = e_{ij}$, on en déduit que $D = E$.

L'égalité $(A + B)C = AC + BC$ se montre de même (attention au format des matrices !).

3. Montrons l'égalité $A(\lambda B) = \lambda(AB)$. Si $A = (a_{ij})_{n,p}$, $B = (b_{ij})_{p,q}$ et $\lambda \in \mathbb{R}$, alors la matrice λB a pour format (p, q) et terme général (λb_{ij}). Donc la matrice $C = A(\lambda B)$ a pour format (n, q) et terme général

$$c_{ij} = \sum_{k=1}^{p} a_{ik}(\lambda b_{kj}) \ .$$

D'autre part, la matrice AB a pour format (n, q) et terme général $(\sum_{k=1}^{p} a_{ik}b_{kj})$. Donc la matrice $D = \lambda(AB)$ a pour format (n, q) et terme général

$$d_{ij} = \lambda \left(\sum_{k=1}^{p} a_{ik}b_{kj} \right) \ = \ c_{ij} \ .$$

Comme les matrices $C = A(\lambda B)$ et $E = \lambda(AB)$ ont même format (n, q) et même terme général $c_{ij} = d_{ij}$, on en déduit l'égalité $A(\lambda B) = \lambda(AB)$.

L'égalité $(\lambda A)B = \lambda(AB)$ se montre de même.

□

Le produit d'une matrice par une autre revient à multiplier la première matrice avec chacune des colonnes de la seconde. Plus précisément :

Proposition 3.8 *Soient A et B deux matrices de formats respectifs (n,p) et (p,q). On note par $c_1,\ldots,c_q$ les q colonnes de la matrice B. Alors les colonnes $c'_1,\ldots,c'_q$ de la matrice AB sont $Ac_1,\ldots,Ac_q$:*

$$A.(c_1\ \ldots\ c_q)\ =\ (Ac_1\ \ldots\ Ac_q)$$

(où Ac_i désigne le produit de la matrice A avec la colonne c_i).

Preuve : Si $E=(e_{ij})_{n,q}=AB$, alors la jème colonne c'_j de la matrice E a pour coordonnées $(e_{1j},\ldots,e_{nj})$ où

$$e_{ij}=\sum_{k=1}^{p}a_{ik}b_{kj}\ .$$

D'autre part, comme le terme général de la matrice colonne c_j est $(b_{ij})_{1\leq i\leq p}$, le terme général $(d_i)_{1\leq i\leq n}$ de la matrice colonne Ac_j est

$$d_i=\sum_{k=1}^{p}a_{ik}b_{kj}\ .$$

On en déduit que $c'_j=Ac_j$ pour tout j.

□

Enfin, chaque colonne d'une matrice se retrouve en multipliant cette matrice par une matrice colonne élémentaire :

Proposition 3.9 *Notons X_j la matrice colonne de format $(p,1)$ dont tous les coefficients sont nuls, sauf celui de la jème ligne qui vaut 1. Si $A\in M_{n,p}$, alors la jème colonne de A est égale au produit AX_j :*

$$A=(AX_1\ \ldots\ AX_p)\ .$$

Preuve : Le terme général de la jème colonne de A est $(a_{ij})_{1\leq i\leq n}$. D'autre part, si $X_j=(x_i)_{1\leq i\leq p}$, le terme général de la matrice colonne $AX_j=(b_i)_{1\leq i\leq n}$ est

$$b_i=\sum_{k=1}^{p}a_{ik}x_k$$

où $x_k=0$ si $k\neq j$ et $x_k=1$ si $k=j$. On en déduit que $b_i=a_{ij}$. Donc la matrice AX_j est égale à la jème colonne de la matrice A.

□

3.4 Transposée d'une matrice

Définition 3.10 *Soit $A = (a_{ij})_{n,p}$ une matrice de $M_{n,p}$. On appelle transposée de A la matrice $A' = (a'_{ij})_{p,n}$ de format (p, n) dont le terme général est*

$$\forall i \in \{1, \ldots, p\},\ \forall j \in \{1, \ldots, n\}, \qquad a'_{ij} = a_{ji}\ .$$

On la note $A' = A^T$.

Proposition 3.11

1. $\forall A \in M_{n,p},\ \forall B \in M_{n,p},\ \forall \lambda \in \mathbb{R}, \qquad (A+B)^T = A^T + B^T$ *et* $(\lambda A)^T = \lambda A^T$.
2. $\forall A \in M_{n,p},\ (A^T)^T = A$.
3. $\forall A \in M_{n,p},\ \forall B \in M_{p,q}, \qquad (AB)^T = B^T\, A^T$.

Preuve :

1. Si $A = (a_{ij})_{n,p}$ et $B = (b_{ij})_{n,p}$, alors la matrice $A + B$ a pour terme général $(a_{ij} + b_{ij})$ et pour format (n, p), et donc la matrice $(A + B)^T$ a pour terme général $(a_{ji} + b_{ji})$ et pour format (p, n). D'autre part, les matrices A^T et B^T ont pour terme général respectivement (a_{ji}) et (b_{ji}), donc la matrice $A^T + B^T$ a pour terme général $(a_{ji} + b_{ji})$ et pour format (p, n). Les matrices $(A + B)^T$ et $A^T + B^T$ ont même format (p, n) et même terme général. Elles sont donc égales. On montre de même l'égalité $(\lambda A)^T = \lambda A^T$.

2. Si $A = (a_{ij})_{n,p}$, la matrice A^T a pour terme général (a_{ji}) et pour format (p, n). Donc la matrice $(A^T)^T$ a pour terme général (a_{ij}) et pour format (n, p). On en déduit l'égalité $(A^T)^T = A$.

3. Si $A = (a_{ij})_{n,p}$ et $B = (b_{ij})_{p,q}$, alors AB a pour format (n, q) et pour terme général $(\sum_{k=1}^{p} a_{ik} b_{kj})$. Par conséquent, la matrice $C = (AB)^T$ a pour format (q, n) et pour terme général

$$c_{ij} = \sum_{k=1}^{p} a_{jk} b_{ki}\ .$$

D'autre part, les matrices A^T et B^T ont pour format respectif (p, n) et (q, p) et pour terme général (a_{ji}) et (b_{ji}). Le produit $D = B^T A^T$ existe donc, a pour format (q, n) et pour terme général

$$d_{ij} = \sum_{k=1}^{p} b_{ki} a_{jk} = c_{ij}$$

Les matrices C et D ont même format (q, n) et même terme général $c_{ij} = d_{ij}$. Elles sont donc égales.

□

Définition 3.12 (Adjointe d'une matrice)
Soit $A = (a_{ij})$ une matrice de $M_{n,p}(C)$ (à coefficients complexes). On appelle adjointe de A la matrice $A' = (a'_{ij})$ de format (p, n) dont le terme général est

$$\forall i \in \{1, \ldots, p\},\ \forall j \in \{1, \ldots, n\}, \qquad a'_{ij} = \overline{a_{ji}}\ .$$

(ici $\overline{z}$ désigne le conjugué du complexe z). On note $A' = A^*$.

4 Les matrices carrées

Nous allons étudier dans ce paragraphe les matrices carrées de format (ou d'ordre) n. Toutes les propriétés vues dans le cas général restent bien entendu valables, mais nous allons voir que ces matrices possèdent en plus des propriétés particulières. L'ensemble des matrices carrées d'ordre n à coefficients réels (resp. complexes) se note $M_n(\mathbb{R})$ (resp. $M_n(C)$) et plus simplement M_n . Comme ci-dessus nous faisons l'exposé dans le cas réel.

4.1 Quelques matrices carrées particulières

- si $A = (a_{ij})_n$ est une matrice carrée d'ordre n, les termes a_{ii} constituent la **diagonale principale** de A.

- une matrice $A = (a_{ij})_n$ est **diagonale** si tous ses termes sont nuls, sauf peut-être ceux de la diagonale principale :

$$\forall (i, j) \in \{1, \ldots, n\}^2, \qquad i \neq j \ \Rightarrow\ a_{ij} = 0\ .$$

- la **matrice identité** d'ordre n, notée I_n est la matrice diagonale dont tous les termes diagonaux sont égaux à 1. Dans le cas où il n'y a pas de risque d'ambiguïté sur l'ordre de la matrice, on la note plus simplement I :

$$\text{Exemple : si } n = 3 \qquad\qquad I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- une matrice A est **scalaire** si c'est une matrice diagonale dont tous les termes diagonaux sont égaux :

$$A \text{ scalaire } \ \Leftrightarrow\ \exists \lambda \in \mathbb{R},\ \ A = \lambda I_n$$

- une matrice A est **triangulaire supérieure** si c'est une matrice dont tous les termes situés en dessous de la diagonale principale sont nuls :

$$\forall (i,j) \in \{1,\ldots,n\}^2, \qquad i > j \;\Rightarrow\; a_{ij} = 0 \; .$$

- une matrice A est **triangulaire inférieure** si c'est une matrice dont tous les termes situés au-dessus de la diagonale principale sont nuls :

$$\forall (i,j) \in \{1,\ldots,n\}^2, \qquad i < j \;\Rightarrow\; a_{ij} = 0 \; .$$

- une matrice A est **symétrique** si elle est égale à sa transposée : $A = A^T$.
- une matrice A **antisymétrique** si elle est égale à l'opposée de sa transposée : $A = -A^T$.
- dans le cas complexe, une matrice A est **auto-adjointe** si elle est égale à son adjointe : $A = A^*$.

4.2 Opérations dans M_n

Le produit de deux matrices de M_n est une matrice de M_n : le produit matriciel est donc dans ce cas une loi interne. Les propriétés de la proposition 3.7 restent bien entendu vraies :

- associativité du produit.
- distributivité du produit par rapport à l'addition.
- $\forall A \in M_n$, $\forall B \in M_n$, $\forall \lambda \in \mathbb{R}$, $A(\lambda B) = (\lambda A)B = \lambda(AB)$.

De plus :

Proposition 4.1
Si I_n est la matrice identité définie ci-dessus, on a :

$$\forall A \in M_n, \;\; AI_n = I_n A = A \; .$$

On dit que I_n est élément neutre pour la multiplication.

Mais encore une fois attention :
- ce produit n'est pas commutatif ($AB \neq BA$ en général)
- ce produit a des diviseurs de zéro : par définition, une matrice A est un **diviseur de zéro** si $A \neq O$ et s'il existe une matrice $B \neq O$ avec $AB = O$ ou $BA = O$.

Preuve de la proposition : Montrons l'égalité $AI_n = A$. Si $A = (a_{ij})_n$ et $I_n = (b_{ij})_n$, alors le produit AI_n a pour format (n, n) et terme général $(\sum_{k=1}^{n} a_{ik}b_{kj})$. D'après la définition de I_n, on a

$$\forall (i,j) \in \{1,\dots,n\}^2, \qquad b_{ij} = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j \end{cases}$$

Donc le terme général de la matrice AI_n est $(\sum_{k=1}^{n} a_{ik}b_{kj} = a_{ij})$, ce qui prouve l'égalité $AI_n = A$.
On montre de même que $I_n A = A$.

□

4.3 Matrices inversibles

Définition 4.2 (Matrices inversibles)
Soit A une matrice de M_n. On dit que A est inversible ou régulière s'il existe une matrice B de M_n telle que :

$$AB = BA = I_n \ .$$

Dans ce cas, la matrice B est unique et s'appelle l'inverse de A. On note $B = A^{-1}$.

Remarque : Notez bien que, si B est l'inverse de A, alors B est inversible et a pour inverse A :

$$B \ = \ A^{-1} \ \Leftrightarrow \ A \ = \ B^{-1} \ .$$

Preuve de l'unicité : Supposons qu'il existe deux matrices B_1 et B_2 telles que

$$AB_1 = B_1A = I_n = AB_2 = B_2A \ .$$

Comme $AB_1 = I_n$, on a, en multipliant cette égalité à gauche par B_2 :

$$B_2(AB_1) = B_2I_n \ .$$

Or

$$B_2(AB_1) = (B_2A)B_1 = I_nB_1 = B_1 \qquad \text{et} \qquad B_2I_n = B_2 \ .$$

On en déduit que $B_1 = B_2$.

□

En fait il suffit, pour que A soit inversible, qu'il existe une matrice B de M_n vérifiant une seule des deux propriétés $AB = I_n$ ou $BA = I_n$. On a alors nécessairement $A^{-1} = B$. Cette propriété remarquable est une conséquence d'un théorème profond que vous verrez au second semestre : le théorème du rang.

Théorème 4.3 *Soit A et B deux matrices de M_n. Si $AB = I_n$, alors A et B sont inversibles et $B = A^{-1}$.*

Preuve (HP) : voir le cours du second semestre.

Proposition 4.4 (Produit de deux matrices inversibles)
Soient A et B deux matrices inversibles de M_n : alors le produit AB est inversible et

$$(AB)^{-1} = B^{-1}A^{-1} .$$

Preuve : Calculons le produit $\left(B^{-1}A^{-1}\right)(AB)$:

$$\begin{array}{rcll} \left(B^{-1}A^{-1}\right)(AB) & = & B^{-1}(A-1A)B & \text{par associativité} \\ & = & B^{-1}I_nB & \text{par définition de } B^{-1} \\ & = & B^{-1}B & \\ & = & I_n & \end{array}$$

On montre de même que

$$(AB)\left(B^{-1}A^{-1}\right) = I_n$$

et on en déduit que AB est inversible et d'inverse $\left(B^{-1}A^{-1}\right)$.

□

Proposition 4.5 (Transposée d'une matrice inversible)
Si A est une matrice carrée inversible, alors A^T est inversible et

$$(A^T)^{-1} = (A^{-1})^T .$$

De même dans le cas complexe, A^* est inversible et $(A^*)^{-1} = (A^{-1})^*$.

Preuve : En transposant l'égalité $AA^{-1} = I_n$, on obtient

$$(A^{-1})^T A^T = (I_n)^T = I_n .$$

De même, en transposant l'égalité $A^{-1}A = I_n$, on obtient

$$A^T(A^{-1})^T = I_n$$

On en déduit que A^T est inversible et que son inverse est $(A^{-1})^T$.
La démonstration pour l'adjointe est identique.

□

Proposition 4.6
Si A est inversible, et si $AB = AC$ (respectivement $BA = CA$) alors $B = C$.

Preuve : On multiplie l'égalité $AB = AC$, à gauche, par A^{-1} pour obtenir

$$A^{-1}(AB) = A^{-1}(AC)$$

Par associativité, on obtient :

$$A^{-1}(AB) = (A^{-1}A)B = I_nB = B$$

De même, $A^{-1}(AC) = C$. Donc $B = C$.
L'autre égalité s'obtient de la même façon, en multipliant à droite l'égalité $BA = CA$ par A^{-1}.

□

Proposition 4.7
Les diviseurs de zéro dans M_n ne sont jamais inversibles.

Preuve : Montrons que, si A est inversible, alors A n'est pas un diviseur de zéro. Soit B une matrice telle que $AB = O$. Comme $O = AO$, on a $AB = AO$ et donc, d'après la proposition précédente : $B = O$. On montre de même que s'il existe une matrice B telle que $BA = O$, alors $B = O$. On en déduit que A n'est pas un diviseur de zéro.

□

5 Matrices et systèmes d'équations linéaires

5.1 Ecriture matricielle d'un système d'équations linéaires

Revenons au système linéaire de n équations à p inconnues donné dans l'introduction :

$$(S) \qquad \left\{ \begin{array}{rcl} a_{11}x_1 + \ldots + a_{1j}x_j + \ldots + a_{1p}x_p & = & b_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots & & \ldots \\ a_{i1}x_1 + \ldots + a_{ij}x_j + \ldots + a_{ip}x_p & = & b_i \\ \ldots\ldots\ldots\ldots\ldots\ldots & & \ldots \\ a_{n1}x_1 + \ldots + a_{nj}x_j + \ldots + a_{np}x_p & = & b_n \end{array} \right.$$

Posons $A = (a_{ij})_{n,p}$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_j \\ \vdots \\ x_p \end{pmatrix}$ et $b = \begin{pmatrix} b_1 \\ \vdots \\ b_j \\ \vdots \\ b_n \end{pmatrix}$. Le système (S) s'écrit matriciellement : $AX = b$.

5.2 Opérations élémentaires sur les lignes d'une matrice

Soit $A = (a_{ij})_{n,p}$ une matrice de $M_{n,p}$. On appelle **transformation de Gauss-Jordan** appliquée à la matrice A l'une quelconque des trois opérations élémentaires suivantes :

1. multiplier la ième ligne par α ($\alpha \neq 0$), opération codée par : $L_i \leftarrow \alpha L_i$
2. échanger les lignes i et j de (S) pour $i \neq j$, opération codée par : $L_i \leftrightarrow L_j$
3. toujours pour $i \neq j$, ajouter à la ligne i la ligne j multipliée par β, opération codée par : $L_i \leftarrow L_i + \beta L_j$ (la condition $\beta \neq 0$ n'étant pas ici imposée).

Notons ϕ l'application de $M_{n,p}$ dans $M_{n,p}$ qui à toute matrice A associe sa transformée par une des transformations de Gauss-Jordan.

Proposition 5.1

$$\forall A \in M_{n,p}, \quad \phi(A) = \phi(I_n)A$$

Autrement dit, pour trouver la transformée de A par l'opération élémentaire sur les lignes considérées, il suffit d'appliquer cette opération élémentaire à la matrice identité d'ordre n (n = nombre de lignes de A) et de faire le produit matriciel de la matrice ainsi obtenue par A.

Preuve :

1. Pour une transformation de la forme $L_i \leftarrow \alpha L_i$: si $A = (a_{kl})_{n,p}$, alors $B = \phi(A)$ a pour terme général $(b_{kl})_{n,p}$ où

$$b_{kl} = \begin{cases} a_{kl} & \text{si } k \neq i \\ \alpha a_{il} & \text{si } k = i \end{cases}$$

Soit $C = \phi(I_n)$ de terme général $C = (c_{kl})_{n,n}$. On a

$$c_{kl} = \begin{cases} 0 & \text{si } k \neq l \\ 1 & \text{si } k = l,\ k \neq i \\ \alpha & \text{si } k = l = i \end{cases}$$

Alors le produit $D = \phi(I_n)A$ a pour format (n, p) et terme général (d_{kl}) où

$$d_{kl} = \sum_{j=1}^{n} c_{kj} a_{jl}$$

Donc d'après la valeur de c_{kl}, on a

$$d_{kl} = \begin{cases} a_{kl} & \text{si } k \neq i \\ \alpha a_{il} & \text{si } k = i \end{cases}$$

En particulier, $d_{kl} = b_{kl}$, c'est-à-dire que les matrices $\phi(A)$ et $\phi(I_n)A$ sont égales.

2. Pour une transformation de la forme $L_i \leftrightarrow L_j$: si $A = (a_{kl})_{n,p}$, alors $B = \phi(A)$ a pour terme général $(b_{kl})_{n,p}$ où

$$b_{kl} = \begin{cases} a_{kl} & \text{si } k \neq i \text{ et } k \neq j \\ a_{jl} & \text{si } k = i \\ a_{il} & \text{si } k = j \end{cases}$$

Soit $C = \phi(I_n)$ de terme général $C = (c_{kl})_{n,n}$. On a

$$c_{kl} = \begin{cases} 0 & \text{si } k \notin \{i, j, l\} \\ 1 & \text{si } k = l, \text{ et } k \neq i, \ k \neq j \\ 0 & \text{si } [k = j, \text{ et } l \neq i] \text{ ou } [k = i \text{ et } l \neq j] \\ 1 & \text{si } [k = j, \text{ et } l = i] \text{ ou } [k = i \text{ et } l = j] \end{cases}$$

Alors le produit $D = \phi(I_n)A$ a pour format (n, p) et terme général (d_{kl}) où

$$d_{kl} = \sum_{m=1}^{n} c_{km} a_{ml}$$

Donc d'après la valeur de c_{kl}, on a

$$d_{kl} = \begin{cases} a_{kl} & \text{si } k \neq i \text{ et } k \neq j \\ a_{jl} & \text{si } k = i \\ a_{il} & \text{si } k = j \end{cases}$$

En particulier, $d_{kl} = b_{kl}$, c'est-à-dire que les matrices $\phi(A)$ et $\phi(I_n)A$ sont égales.

3. Pour une transformation de la forme $L_i \leftarrow L_i + \beta L_j$: si $A = (a_{kl})_{n,p}$, alors $B = \phi(A)$ a pour terme général $(b_{kl})_{n,p}$ où

$$b_{kl} = \begin{cases} a_{kl} & \text{si } k \neq i \\ a_{il} + \beta a_{jl} & \text{si } k = i \end{cases}$$

Soit $C = \phi(I_n)$ de terme général $C = (c_{kl})_{n,n}$. On a

$$c_{kl} = \begin{cases} 0 & \text{si } k \neq l \text{ et } k \neq i \\ 1 & \text{si } k = l \\ \beta & \text{si } k = i \text{ et } l = j \end{cases}$$

Alors le produit $D = \phi(I_n)A$ a pour format (n, p) et terme général (d_{kl}) où

$$d_{kl} = \sum_{m=1}^{n} c_{km} a_{ml}$$

Donc d'après la valeur de c_{kl}, on a

$$d_{kl} = \begin{cases} a_{kl} & \text{si } k \neq i \\ a_{il} + \beta a_{jl} & \text{si } k = i \end{cases}$$

En particulier, $d_{kl} = b_{kl}$, c'est-à-dire que les matrices $\phi(A)$ et $\phi(I_n)A$ sont égales.

□

Corollaire 5.2 *Soient $\phi_1, \ldots, \phi_k$ une suite de transformations de Gauss-Jordan et A une matrice. Alors*

$$\phi_1 \circ \ldots \circ \phi_k(A) = \phi_1(I_n) \ldots \phi_k(I_n)A \ .$$

Preuve : On fait la démonstration par récurrence sur k. Pour $k = 1$, nous avons vu à la proposition 5.1 que c'est vrai. On suppose que le résultat est vrai jusqu'au rang k. Alors, si $\phi_1, \ldots, \phi_{k+1}$ une suite de transformations de Gauss-Jordan, on a

$$\phi_1 \circ \ldots \circ \phi_{k+1}(A) = \phi_1(I_n).\phi_2 \circ \ldots \circ \phi_{k+1}(A)$$

d'après la proposition 5.1. L'hypothèse de récurrence affirme que

$$\phi_2 \circ \ldots \circ \phi_{k+1}(A) = \phi_2(I_n) \ldots \phi_{k+1}(I_n)A \ .$$

Par conséquent,

$$\phi_1 \circ \ldots \circ \phi_{k+1}(A) = \phi_1(I_n).\phi_2(I_n) \ldots \phi_{k+1}(I_n)A \ ,$$

ce qui prouve le résultat au rang k.
Par récurrence, on en déduit que le résultat est vrai pour tout k.

□

5.3 Méthode pratique de calcul de l'inverse d'une matrice

Pour calculer l'inverse d'une matrice $A = (a_{ij})$, on écrit le tableau à n lignes et $2n$ colonnes obtenu en juxtaposant la matrice A et la matrice I_n à sa droite par exemple :

a_{11}	$\ldots$	$\ldots$	a_{1n}	1	0	$\ldots$	0
$\ldots$	$\ldots$	$\ldots$	$\ldots$	0	1	$\ldots$	$\vdots$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\vdots$	$\ldots$	1	0
a_{n1}	$\ldots$	$\ldots$	a_{nn}	0	$\ldots$	0	1

On effectue les mêmes transformations de Gauss-Jordan simultanément sur les deux tableaux jusqu'à ce qu'on arrive au tableau suivant :

1	0	$\ldots$	0	α_{11}	$\ldots$	$\ldots$	α_{1n}
0	1	$\ldots$	$\vdots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$\vdots$	$\ldots$	1	0	$\ldots$	$\ldots$	$\ldots$	$\ldots$
0	$\ldots$	0	1	α_{n1}	$\ldots$	$\ldots$	α_{nn}

La matrice A^{-1} cherchée est la matrice (α_{ij}) obtenue à la droite du nouveau tableau. En effet :

Proposition 5.3 *Soient $\phi_1, \ldots, \phi_k$ une suite de transformations de Gauss-Jordan et A une matrice. Si*

$$\phi_1 \circ \ldots \circ \phi_k(A) = I_n \ ,$$

alors A est inversible et

$$A^{-1} = \phi_1(I_n) \ldots \phi_k(I_n) \ .$$

Preuve : Comme, d'après le corollaire 5.2,

$$\phi_1 \circ \ldots \circ \phi_k(A) = \phi_1(I_n) \ldots \phi_k(I_n))A \ ,$$

on en déduit que $BA = I_n$, où

$$B = \phi_1(I_n) \ldots \phi_k(I_n)) \ .$$

Alors le lemme 4.3 permet de conclure que B est l'inverse de A.

□