Algèbre 1
MIAS 1

Thierry Cuesta

26 septembre 2003

Le présent cours trouve sa source dans les notes que j'avais rédigées lors du premier semestre de l'année universitaire 2001/2002, alors que j'enseignais pour la première fois l'algèbre en DEUG MIAS. Les trois heures hebdomadaires dédiées à cet enseignement dans l'emploi du temps des étudiants, ne m'avaient pas permis de justifier chacun des énoncés. J'avais le sentiment d'avoir bâclé une bonne partie des démonstrations, d'avoir laissé de côté une part trop importante du formalisme sans doute nécessaire, afin de ménager suffisamment de temps pour traiter les exercices des TD. Ces frustrations conjuguées à : une panne de voiture durant l'été 2002, l'achat d'un ordinateur, l'envie d'apprivoiser le « traitement de texte » LaTeX, ont eu pour conséquence la rédaction de la première version de ce cours.

La version actuelle de ce cours n'est que la version révisée et (peu) augmentée de la version initiale. Il est probable que quelques erreurs subsistent, en dépit des relectures auxquelles je me suis livré. Toute personne débusquant une erreur, ou mieux encore : corrigeant une erreur, se verra attribuer une forte récompense... pour peu que le budget "récompenses" soit enfin voté en conseil d'administration. Vous pouvez m'envoyer vos commentaires, suggestions, corrections, etc. par e-mail, à l'adresse : `Thierry.Cuesta@ac-creteil.fr`.

J'espère que ce document est auto-suffisant. Si mon but est atteint, une lecture attentive devrait permettre, à ceux qui s'y astreindront, d'acquérir le contenu théorique du tout premier semestre d'algèbre du DEUG MIAS. Il ne s'agit cependant pas d'un encouragement à ne plus venir à l'université assister aux cours ! Mieux vaut avoir des versions différentes d'une même notion ; la version « live » est interactive, et en principe moins abstraite et plus condensée que la présente version. La réponse d'un enseignant à une question que vous lui poserez vous fera gagner un temps précieux pour la compréhension d'un chapitre. Une fois fixé sur le papier, un cours ne saurait réagir à vos difficultés comme le fera votre professeur. N'oubliez pas que rare sont les enseignants condamnés pour cannibalisme, et qu'ils sont en général soucieux de votre réussite.

Je remercie Lionel Girard qui m'a tant vanté les mérites de TeX que je n'ai pu faire autrement que de m'y essayer, les « chefs d'orchestre » Étienne Sandier et Raphaël Danchin pour leur ouverture d'esprit favorisant les initiatives chez leurs collaborateurs, Clothilde Melot qui m'a poussé vers l'ALU avant même d'avoir pris connaissance du contenu de ce cours, les membres de l'équipe de mathématiques de l'université Paris XII Val-de-Marne avec lesquels je travaille depuis 1998 et qui m'ont accordé leur confiance.

Thierry Cuesta

Table des matières

Chapitre 1

Introduction

1.1 Ensembles

1.1.1 Ensembles

Nous allons dans ce court chapitre, examiner quelques objets mathématiques liés à la structure d'ensemble. Le propos ne sera pas d'exposer une théorie [1] (axiomatique?) des ensembles. Les prétentions théoriques seront plus que restreintes. Seule une idée intuitive de la notion d'ensemble sera utilisée. Si vous parvenez à donner son sens à une phrase comme : « Je suis un élément de l'ensemble des étudiants du DEUG MIAS », vous disposez d'un bagage suffisant pour entamer la lecture de ce chapitre. Certains ensembles auront un nombre fini d'éléments et seront appelés : ensembles finis. On rappelle que « l'élément a appartient à l'ensemble $\mathcal{A}$ » s'écrit : $a \in \mathcal{A}$, et que « l'élément a n'appartient pas à l'ensemble $\mathcal{A}$ » s'écrit : $a \notin \mathcal{A}$.

Définition et notation 1.1.1 (Sous-ensemble) *On dit que $\mathcal{B}$ est un sous-ensemble de $\mathcal{A}$, si tous les éléments de $\mathcal{B}$ sont des éléments de $\mathcal{A}$. On écrit alors : $\mathcal{B} \subset \mathcal{A}$. (Lire : $\mathcal{B}$ est inclus dans $\mathcal{A}$).*

On rencontre également, à la place de $\mathcal{B} \subset \mathcal{A}$, la notation $\mathcal{A} \supset \mathcal{B}$ qui a la même signification. On remarque que $a \in \mathcal{A}$ équivaut à $\{a\} \subset \mathcal{A}$. Les accolades sont utilisées pour noter les ensembles dont on exhibe les éléments. Par exemple $\{a, b\}$ est l'ensemble [2] dont les deux éléments sont a et b. Dans $\{a, a\}$ il n'y a pas deux éléments mais un seul [3], et on écrit $\{a\}$ au lieu de $\{a, a\}$.

Définition et notation 1.1.2 *Soient $\mathcal{A}$ et $\mathcal{B}$ des ensembles. $\mathcal{A} \setminus \mathcal{B}$ est l'ensemble des éléments de $\mathcal{A}$ qui n'appartiennent pas à $\mathcal{B}$.*

Définition 1.1.3 (Complémentaire) *Soit $\mathcal{A}$ un ensemble et $\mathcal{B}$ un sous-ensemble de $\mathcal{A}$. $\mathcal{A} \setminus \mathcal{B}$ est le complémentaire de $\mathcal{B}$ dans $\mathcal{A}$.*

Définition et notation 1.1.4 (Ensemble vide) *L'unique ensemble n'ayant aucun élément : l'ensemble vide, est noté : $\emptyset$.*

On remarque que l'ensemble vide est un sous-ensemble de n'importe quel ensemble. En effet, soit $\mathcal{A}$ un ensemble ; $\emptyset \subset \mathcal{A}$ si et seulement si tout élément de $\emptyset$ est un élément de $\mathcal{A}$. Or, comme $\emptyset$ n'a pas d'élément, on a vite fait de vérifier que tout élément de $\emptyset$ est un élément de $\mathcal{A}$.

Définition et notation 1.1.5 (Union) *La réunion des ensembles $\mathcal{A}$ et $\mathcal{B}$ est l'ensemble, noté : $\mathcal{A} \cup \mathcal{B}$, des éléments qui appartiennent à $\mathcal{A}$ ou [4] à $\mathcal{B}$.*

Définition et notation 1.1.6 (Intersection) *L'intersection des ensembles $\mathcal{A}$ et $\mathcal{B}$ est l'ensemble, noté : $\mathcal{A} \cap \mathcal{B}$, des éléments qui appartiennent à $\mathcal{A}$ et aussi à $\mathcal{B}$.*

1. [2] est une bonne introduction au monde de la théorie des ensembles et de la logique mathématique.
2. Un ensemble à deux éléments est une paire.
3. Un ensemble à un seul élément est un singleton.
4. Le « ou » de cette définition est un « ou » inclusif. Il signifie : soit l'un, soit l'autre, soit les deux.

On remarque que pour tout ensemble $\mathcal{A}$ et tout ensemble $\mathcal{B}$:

$$\mathcal{A} \cap \mathcal{B} \subset \mathcal{A} \subset \mathcal{A} \cup \mathcal{B}.$$

Définition et notation 1.1.7 (Union) *Soit I un ensemble (ensemble d'indices). Pour tout $i \in I$, $\mathcal{A}_i$ est un ensemble. Alors $\bigcup_{i\in I} \mathcal{A}_i$ est l'ensemble des éléments x pour lesquels il existe $i_0 \in I$ tel que $x \in \mathcal{A}_{i_0}$.*

Définition et notation 1.1.8 (Intersection) *Soit I un ensemble (ensemble d'indices), $I \neq \emptyset$. Pour tout $i \in I$, $\mathcal{A}_i$ est un ensemble. Alors $\bigcap_{i\in I} \mathcal{A}_i$ est l'ensemble des éléments x tels que pour tout $i \in I$, $x \in \mathcal{A}_i$.*

Si dans la définition 1.1.7, $I = \emptyset$, alors $\bigcup_{i\in\emptyset} \mathcal{A}_i = \emptyset$. Mais dans la définition 1.1.8, on ne peut avoir [5] $I = \emptyset$.

Définition et notation 1.1.9 (Ensemble des parties) *Soit $\mathcal{A}$ un ensemble. L'ensemble des parties de $\mathcal{A}$ est l'ensemble dont les éléments sont les sous-ensembles de $\mathcal{A}$. Cet ensemble est noté : $\mathcal{P}(\mathcal{A})$.*

Exemples : $\mathcal{P}(\emptyset) = \{\emptyset\}$. Si $\mathcal{A} = \{a\}$, alors $\mathcal{P}(\mathcal{A}) = \{\emptyset, \{a\}\}$. Si $\mathcal{A} = \{a, b\}$, alors $\mathcal{P}(\mathcal{A}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

Définitions et notations 1.1.10 (Quantificateurs) *Soit $\mathfrak{P}(x)$ une propriété mathématique dépendant d'un objet mathématique x. La suite de symboles [6] :*

$$(\forall x \in \mathcal{A}) \quad \mathfrak{P}(x)$$

se lit : « Pour tout x élément de $\mathcal{A}$, $\mathfrak{P}(x)$ » ; autrement dit : pour tout x, si $x \in \mathcal{A}$ alors la propriété $\mathfrak{P}(x)$ est vraie.
La suite de symboles [7] :

$$(\exists x \in \mathcal{A}) \quad \mathfrak{P}(x)$$

se lit : « Il existe x élément de $\mathcal{A}$, $\mathfrak{P}(x)$; autrement dit : il existe x, $x \in \mathcal{A}$ et $\mathfrak{P}(x)$ est vraie.
$\forall$ est le quantificateur universel, $\exists$ est le quantificateur existentiel.

Remarque importante : Si $\mathcal{A} = \emptyset$, alors quelle que soit la propriété $\mathfrak{P}(x)$, l'énoncé : « $(\forall x \in \mathcal{A}) \quad \mathfrak{P}(x)$ » est vrai, et l'énoncé : « $(\exists x \in \mathcal{A}) \quad \mathfrak{P}(x)$ » est faux.

Notation 1.1.11 *Soit $\mathfrak{P}(x)$ une propriété mathématique dépendant de l'objet mathématique x. L'ensemble des éléments a de $\mathcal{A}$, tels que $\mathfrak{P}(a)$ est vraie, se note :*

$$\{a \in \mathcal{A} \mid \mathfrak{P}(a)\}.$$

C'est un sous-ensemble de $\mathcal{A}$.

1.1.2 Applications

La notion d'application est présentée de façon détaillée dans l'excellent [5], ainsi que dans tout ouvrage de théorie des ensembles ou de logique mathématique, comme dans le non moins excellent, mais moins abordable, [3].

Définition et notation 1.1.12 (Couple) *Soient a et b des éléments d'un ensemble $\mathcal{E}$. On définit le « couple a b », noté (a, b), par :*

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

On remarque que $\{a\}$ et $\{a, b\}$ sont des sous-ensembles de $\mathcal{E}$; donc, $\{a\}$ et $\{a, b\}$ sont des éléments de $\mathcal{P}(\mathcal{E})$, et finalement $(a, b) \in \mathcal{P}(\mathcal{P}(\mathcal{E}))$.

Proposition 1.1.1 *Soient a, b, a' et b' des éléments d'un ensemble $\mathcal{E}$. $(a, b) = (a', b')$ si et seulement si $a = a'$ et $b = b'$.*

5. Le cas pathologique pour l'intersection : $I = \emptyset$, donnerait naissance à l'ensemble de tous les ensembles... qui n'existe pas !
6. $\forall x\,(x \in \mathcal{A} \Rightarrow \mathfrak{P}(x))$ serait plus convenable mais moins pratique.
7. $\exists x\,(x \in \mathcal{A} \wedge \mathfrak{P}(x))$ est plus correct (voir la bible des logiciens : René Cori, Daniel Lascar, *Cours de logique mathématique*, Masson, 1993).

Démonstration 1.1.1 Si $a = a'$ et $b = b'$ alors les ensembles (a, b) et (a', b') ont les mêmes éléments ; ils sont donc égaux.
Réciproquement, supposons $(a, b) = (a', b')$. Si $a = b$, alors $\{a, b\} = \{a\}$ et $(a, b) = (a, a) = \{\{a\}\}$. Comme (a, a) n'a qu'un élément et $(a, a) = (a, b) = (a', b')$, (a', b') n'a qu'un seul élément ; autrement dit : $\{a', b'\} = \{a'\}$, ce qui n'est possible que si $a' = b'$. Comme $(a, a) = (a', a')$, ces ensembles à un élément ont le même élément, donc $\{a\} = \{a'\}$ et finalement $a = a'$. Si $a \neq b$ alors (a, b) a deux éléments, donc (a', b') a aussi deux éléments et $a' \neq b'$. Dans (a, b), comme dans (a', b'), il y un ensemble à un élément et un ensemble à deux éléments. Puisque les couples sont égaux, il y a égalité des ensembles à un élément : $\{a\} = \{a'\}$, et donc $a = a'$, et il y a aussi égalité des ensembles à deux éléments : $\{a, b\} = \{a', b'\}$, et donc $b = b'$.

Définition et notation 1.1.13 (Ensemble produit) *Soient $\mathcal{A}$ et $\mathcal{B}$ des ensembles. L'ensemble des couples (a, b) tels que $a \in \mathcal{A}$ et $b \in \mathcal{B}$ est le produit des ensembles $\mathcal{A}$ et $\mathcal{B}$. Il est noté :*

$$\mathcal{A} \times \mathcal{B}$$

(lire « $\mathcal{A}$ croix $\mathcal{B}$ »).

Définition et notation 1.1.14 (Application) *Soient $\mathcal{A}$ et $\mathcal{B}$ des ensembles. On dit que le sous-ensemble f de $\mathcal{A} \times \mathcal{B}$, est une application de $\mathcal{A}$ vers $\mathcal{B}$, lorsque :*

- *pour tout a dans $\mathcal{A}$, il existe b dans $\mathcal{B}$ tel que $(a, b) \in f$;*
- *pour tout a dans $\mathcal{A}$, si (a, b) et (a, b') appartiennent à f, alors $b = b'$.*

La notation $f : \mathcal{A} \to \mathcal{B}$ se lit : « f est une application de $\mathcal{A}$ vers $\mathcal{B}$ ».

Des exemples bien connus d'applications sont les fonctions étudiées au lycée, qui sont des applications d'un intervalle, ou d'une réunion d'intervalles, de $\mathbb{R}$ vers $\mathbb{R}$.

Définition et notation 1.1.15 (Image) *Soit f une application de $\mathcal{A}$ vers $\mathcal{B}$. Soit a un élément de $\mathcal{A}$. L'unique*[8] *élément b de $\mathcal{B}$ tel que (a, b) appartient à f, s'appelle l'image de a par l'application f et se note $f(a)$.*

Définition 1.1.16 (Antécédent) *Soit $f : \mathcal{A} \to \mathcal{B}$. Soit b un élément de $\mathcal{B}$. Les éléments a de $\mathcal{A}$ tels $f(a) = b$ sont les antécédents de b. S'il n'existe aucun élément de $\mathcal{A}$ ayant pour image b par f, on dit alors que b n'a pas antécédent par f.*

Notation 1.1.17 *Soit $f : \mathcal{A} \to \mathcal{B}$. $a \overset{f}{\mapsto} b$, ou plus simplement $a \mapsto b$, lorsque f est sous-entendue, signifie : a a pour image b par f.*

Cette notation est souvent utilisée pour les fonctions. Elle permet, lorsque l'on connait le calcul explicite de l'image, de le faire apparaître à droite de la flèche $\mapsto$. Par exemple, si on appelle f l'application de $\mathbb{R}$ vers $\mathbb{R}$ qui à un nombre réel associe son carré, on note l'ensemble de ces renseignements sous la forme abstraite suivante :

$$f : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2.$$

Notations 1.1.18 *Soient $\mathcal{A}$ et $\mathcal{B}$ des ensembles, soit f une application de $\mathcal{A}$ vers $\mathcal{B}$, soit A un sous-ensemble de $\mathcal{A}$, et soit B un sous-ensemble de $\mathcal{B}$. On note $f(A)$ l'ensemble des éléments de $\mathcal{B}$ ayant un antécédent par f dans A ; autrement dit : $f(A)$ est l'ensemble des images par f des éléments de A.*

$$f(A) = \{b \in \mathcal{B} \mid (\exists a \in A) \quad f(a) = b\}.$$

On note $f^{-1}(B)$ l'ensemble des éléments de $\mathcal{A}$ dont l'image par f appartient à B ; autrement dit : $f^{-1}(B)$ est l'ensemble des antécédents par f des éléments de B.

$$f^{-1}(B) = \{a \in \mathcal{A} \mid f(a) \in B\}.$$

Définition 1.1.19 (Injection) *On dit que l'application f de $\mathcal{A}$ vers $\mathcal{B}$ est injective (est une injection), lorsque tout élément de $\mathcal{B}$ possède au plus un antécédent dans $\mathcal{A}$ par f.*

Définition 1.1.20 (Surjection) *On dit que $f : \mathcal{A} \to \mathcal{B}$ est surjective, lorsque tout élément de $\mathcal{B}$ possède au moins un antécédent par f.*

8. Voir la définition 1.1.14

Définition 1.1.21 (Bijection) *On dit que $f : \mathcal{A} \to \mathcal{B}$ est bijective, lorsque f est à la fois injective et surjective.*

Notation 1.1.22 *Soient $\mathcal{A}$ et $\mathcal{B}$ des ensembles. L'ensemble des applications de $\mathcal{A}$ vers $\mathcal{B}$ se note : $\mathcal{B}^{\mathcal{A}}$.*

Soit $\mathcal{E}$ un ensemble. Notons [9] 2 l'ensemble $\{0, 1\}$. On note alors : $\mathcal{E}^2$, l'ensemble des applications de 2 dans $\mathcal{E}$. Soit $\phi : \mathcal{E} \times \mathcal{E} \to \mathcal{E}^2$ qui associe au couple (a, b) l'application $f : 2 \to \mathcal{E}$ définie par $f(0) = a$ et $f(1) = b$. ϕ est une bijection de $\mathcal{E} \times \mathcal{E}$ sur $\mathcal{E}^2$. Les notations $\mathcal{E} \times \mathcal{E}$ et $\mathcal{E}^2$ seront, à cause de la bijection ϕ, indifféremment employées.

1.1.3 Lois internes

Considérons un ensemble non vide $\mathcal{E}$.

Définition 1.1.23 (Loi interne) *La loi interne $*$ sur $\mathcal{E}$ est une application [10] qui à des éléments a et b de $\mathcal{E}$ associe un élément de $\mathcal{E}$ noté $a * b$.*

Définition 1.1.24 (Associativité) *On dit que la loi $*$ est associative lorsque $a * (b * c) = (a * b) * c$ pour tout a, tout b et tout c, éléments de $\mathcal{E}$.*

Définition 1.1.25 (Commutativité) *On dit que la loi $*$ est commutative lorsque $a * b = b * a$ pour tout $a \in \mathcal{E}$ et tout $b \in \mathcal{E}$.*

Définition 1.1.26 (Élément neutre) *On dit que e est un élément neutre de la loi $*$ lorsque $e * a = a * e = a$ pour tout a dans $\mathcal{E}$.*

Proposition 1.1.2 (Unicité de l'élément neutre) *Si e et e' sont éléments neutres pour $*$, alors $e = e'$.*

Démonstration 1.1.2 Comme e est élément neutre, on a : $e * e' = e'$. Comme e' est élément neutre, on a : $e * e' = e$. D'où le résultat.

Définition 1.1.27 (Inverse) *On dit que a possède un inverse (on dit : un opposé, quand la loi est appelée somme ou addition) lorsqu'il existe b tel que*

$$a * b = b * a = e$$

où e désigne l'élément neutre de $*$.

Exercice 1.1.1 (Unicité de l'inverse) *Démontrer que si b et c sont des inverses de a, alors $b = c$.*

Définition 1.1.28 (Distributivité) *Soient $*$ et $\bullet$ deux lois internes commutatives sur $\mathcal{E}$. On dit que $*$ est distributive par rapport à $\bullet$ lorsque :*

$$(\forall a \in \mathcal{E})(\forall b \in \mathcal{E})(\forall c \in \mathcal{E}) \quad a * (b \bullet c) = (a * b) \bullet (a * c)$$

Exemple : La somme et le produit sont deux lois internes sur $\mathbb{Q}$. Elles sont associatives et commutatives. L'élément neutre de la somme est : 0. Celui du produit est : 1. Tout élément a de $\mathbb{Q}$ admet un opposé, noté : $-a$, pour la somme, et tout élément a non nul de $\mathbb{Q}$ admet un inverse, noté : $\frac{1}{a}$ pour le produit. Comme pour tout a, tout b et tout c dans $\mathbb{Q}$: $a(b + c) = ab + ac$, le produit est distributif par rapport à la somme.
Autre exemple : Considérons $\mathbb{Z}$ muni de la somme et du produit usuels. Ces lois internes sont commutatives et associatives. 0 est l'élément neutre de la somme, 1 celui du produit. Tout élément possède un opposé (pour la somme). Les seuls éléments inversibles (pour le produit) sont : -1 et 1. Le produit est distributif par rapport à la somme.

9. La construction ensembliste traditionnelle des nombres entiers naturels consiste à poser : $0 = \emptyset$ et $n + 1 = n \cup \{n\}$ pour tout $n \neq 0$. Ce point de vue donne : $1 = 0 \cup \{0\} = \{0\}$ et $2 = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$.
10. C'est donc une application de $\mathcal{E} \times \mathcal{E}$ dans $\mathcal{E}$.

1.2 Récurrence

Un outil sera fréquemment utilisé : la démonstration par récurrence.
De quoi s'agit ?
C'est un principe de démonstration d'une infinité de propriétés en un nombre fini d'étapes. On considère les propriétés $\mathcal{P}_n$, avec n décrivant l'ensemble des nombres entiers naturels : $\mathbb{N}$. Pour un nombre entier donné n, la propriété $\mathcal{P}_n$ est soit vraie, soit fausse. Par exemple, la propriété $\mathcal{P}_n$: "l'entier n est pair", est vraie lorsque n est pair, et fausse lorsque n est impair.
La démonstration par récurrence fonctionne suivant le schéma :

il existe un entier n_0 tel que :

- $\mathcal{P}_{n_0}$ est vraie ;
- pour tout entier $n \geqslant n_0$, si $\mathcal{P}_n$ est vraie alors $\mathcal{P}_{n+1}$ est vraie.

La conclusion est alors : pour tout entier $n \geqslant n_0$, $\mathcal{P}_n$ est vraie.

Examinons la validité de ce principe de démonstration.
Supposons remplies les hypothèses, à savoir : "il existe un entier n_0 tel que $\mathcal{P}_{n_0}$ est vraie et, pour tout entier $n \geqslant n_0$, si $\mathcal{P}_n$ est vraie alors $\mathcal{P}_{n+1}$ est vraie". Supposons que la conclusion proposée : "pour tout entier $n \geqslant n_0$, $\mathcal{P}_n$ est vraie", soit fausse. Alors, il existe au moins un entier k supérieur ou égal à n_0 tel que $\mathcal{P}_k$ est fausse.
Soit m le plus petit des entiers $k \geqslant n_0$ tels que $\mathcal{P}_k$ est fausse. Ce nombre m ne peut être n_0, car, par hypothèse, $\mathcal{P}_{n_0}$ est vraie. De $m > n_0$, on déduit : $m - 1 \geqslant n_0$. Comme m est le plus petit des entiers $k \geqslant n_0$ tel que $\mathcal{P}_k$ est fausse, on en déduit que $\mathcal{P}_{m-1}$ est vraie. Or, pour $n \geqslant n_0$, si $\mathcal{P}_n$ est vraie, alors $\mathcal{P}_{n+1}$ est vraie. On aboutit donc à une contradiction puisque de $\mathcal{P}_{m-1}$ vraie, on doit en déduire $\mathcal{P}_m$ vraie, alors que $\mathcal{P}_m$ est fausse. Quelle est la source de cette contradiction ? C'est le fait d'avoir supposé l'existence d'au moins un entier k supérieur ou égal à n_0 et tel que $\mathcal{P}_k$ soit fausse.
Il existe une variante de ce principe de démonstration qui consiste à remplacer dans les hypothèses "pour tout entier $n \geqslant n_0$, si $\mathcal{P}_n$ est vraie alors $\mathcal{P}_{n+1}$ est vraie", par "pour tout entier $n \geqslant n_0$, si $\mathcal{P}_k$ est vraie pour chaque entier k dans $[n_0, n]$, alors $\mathcal{P}_{n+1}$ est vraie".

1.3 Analyse combinatoire

Définition et notation 1.3.1 *Soit $n \in \mathbb{N}$.*
La notation $n!$ se lit : « factorielle n ».
On pose : $n! = \begin{cases} 1 \times 2 \times \cdots \times (n-1) \times n & \text{si } n \neq 0 \\ 1 & \text{si } n = 0 \end{cases}$

Exercice 1.3.1 *On définit par récurrence la notation $Fac(n)$, pour tout nombre entier naturel n, de la manière suivante :*
Fac(0)=1
Fac(n+1)=(n+1)Fac(n)
Montrer [11] *que, pour tout $n \in \mathbb{N}$: $Fac(n) = n!$.*

Notation 1.3.2 *Soient a et b des nombres réels. On note $[\![a, b]\!]$ l'ensemble* [12] $\mathbb{N} \cap [a, b]$.

1.3.1 Permutations

On considère un ensemble fini $\mathcal{E}$ ayant n éléments ($n \in \mathbb{N}$). De combien de façons différentes peut-on ranger tous les éléments de $\mathcal{E}$?
Pour attribuer la première place, on dispose de n choix. Une fois choisi l'élément de $\mathcal{E}$ qui occupe la première place, il reste dans $\mathcal{E}$, $n-1$ éléments parmi lesquels on en choisit un pour occuper la deuxième place. A chacun des n choix du premier élément, correspond $n-1$ choix pour le second. Il y a donc $n(n-1)$ façons différentes de ranger deux éléments de $\mathcal{E}$. Il reste, à ce stade, $n-2$ éléments dans $\mathcal{E}$. On continue d'ordonner, de ranger, ainsi tous les éléments de $\mathcal{E}$.

Définition 1.3.3 (Permutations) *Chaque rangement de tous les éléments d'un ensemble à n éléments, est ce qu'on appelle une permutation dans un ensemble à n éléments.*

11. Un premier essai de démonstration par récurrence s'impose !
12. Cette notation n'étant pas une notation normalisée, il faudra la définir si vous l'utilisez dans un devoir.

Proposition 1.3.1 *Soit $n \in \mathbb{N}$. Il y a $n!$ permutations dans un ensemble à n éléments.*

Démonstration 1.3.1 Notons $\mathcal{P}_n$ la propriété : « il y a $n!$ permutations dans un ensemble à n éléments ». Montrons, par récurrence sur n, que $\mathcal{P}_n$ est vraie pour tout nombre entier naturel n. Pour $n = 0$, la propriété est vérifiée, car il n'y a qu'une façon de ranger les éléments d'un ensemble qui n'en a pas : ne rien faire. (Si ce point de vue vous embarrasse, commencez pas examiner que $\mathcal{P}_1$ est vraie).
Hypothèse de récurrence : $\mathcal{P}_n$ est vraie.
Montrons qu'alors $\mathcal{P}_{n+1}$ est vraie.
Considérons un ensemble à $n+1$ éléments. Il y a $n+1$ façons différentes de choisir un élément parmi $n+1$ éléments. Une fois cet élément choisi, il reste à ranger les n éléments restants. Il y a donc $(n+1)\times$ « le nombre de permutations dans un ensemble à n éléments » façons différentes de ranger $n+1$ éléments. Ce qui donne, en appliquant l'hypothèse de récurrence : $(n+1) \times n! = (n+1)!$ permutations sur un ensemble à $n+1$ éléments. D'où la validité de $\mathcal{P}_{n+1}$.
On en déduit que $\mathcal{P}_n$ est vraie pour tout $n \in \mathbb{N}$.

1.3.2 Arrangements

On considère un ensemble fini $\mathcal{E}$ ayant n éléments ($n \in \mathbb{N}$).
On souhaite ici attribuer p places ($p \leqslant n$). La situation de départ est identique à celle du problème des permutations. La seule différence est qu'on n'épuise pas forcément $\mathcal{E}$ puisqu'on ne range que p éléments.

Définition et notation 1.3.4 (Arrangements) *Chaque rangement de p éléments dans un ensemble à n éléments ($p \in [\![0, n]\!]$), est un arrangement de p éléments parmi n. Le nombre d'arrangements de p éléments parmi n se note : A_n^p.*

Proposition 1.3.2 *Soient n et p deux éléments de $\mathbb{N}$ tels que $p \in [\![0, n]\!]$.*

$$A_n^p = \frac{n!}{(n-p)!}$$

Démonstration 1.3.2 (Trame de démonstration)
On montre que : $A_n^p = n \times (n-1) \times \cdots \times (n-(p-1))$.
Comme $n \times (n-1) \times \cdots \times (n-(p-1)) = \frac{n \times (n-1) \times \cdots \times (n-(p-1)) \times (n-p) \times (n-(p+1) \times \cdots \times 2}{(n-p) \times (n-(p+1) \times \cdots \times 2}$, on en déduit la proposition.

1.3.3 Combinaisons

On considère un ensemble fini $\mathcal{E}$ ayant n éléments ($n \in \mathbb{N}$).
On souhaite cette fois s'intéresser aux sous-ensembles à p éléments d'un ensemble à n éléments ($p \leqslant n$).

Définition et notation 1.3.5 (Combinaisons) *Un sous-ensemble de $\mathcal{E}$ à p éléments s'appelle aussi : une combinaison de p éléments parmi n éléments. Le nombre de sous ensembles à p éléments, d'un ensemble à n éléments, se note [13] : C_n^p.*

Proposition 1.3.3 *Soient $n \in \mathbb{N}$ et $p \in [\![0, n]\!]$.*

$$C_n^p = \frac{n!}{(n-p)!\,p!}$$

Démonstration 1.3.3 Considérer un sous-ensemble à p éléments dans un ensemble à n éléments, c'est choisir p éléments parmi n. Ceci nous rapproche donc de la situation déjà examinée des arrangements de p éléments dans un ensemble à n éléments. La différence est qu'ici, l'ordre dans lequel les p éléments sont choisis n'intervient plus. Il y a $p!$ permutations dans un ensemble à p éléments. Donc, à chaque sous-ensemble à p éléments, correspond $p!$ arrangements différents. On en déduit : $p!\,C_n^p = A_n^p$.

Exercice 1.3.2 *Soient n et p deux éléments de $\mathbb{N}$ tels que $p \leqslant n$.*
Montrer que : $C_n^{n-p} = C_n^p$.

13. On rencontre parfois la notation : $\binom{n}{p}$ à la place de C_n^p.

Triangle de Pascal

Proposition 1.3.4 $(\forall n \in \mathbb{N} \setminus \{0\})(\forall p \in [\![0, n-1]\!]) \quad C_{n+1}^{p+1} = C_n^p + C_n^{p+1}$

Démonstration 1.3.4 Soit [14] $\mathcal{E}$ un ensemble à $n+1$ éléments. Considérons un élément de $\mathcal{E}$, et notons α cet élément. Les sous-ensembles de $\mathcal{E}$ à $p+1$ éléments sous alors de deux types :
-ceux qui comptent α parmi leurs éléments,
-ceux qui ne contiennent pas α.
Combien y a-t-il de sous-ensembles de $\mathcal{E}$ à $p+1$ éléments, et contenant α ? Puisqu'α a déjà été choisi, il reste p éléments à choisir parmi les n éléments restant dans $\mathcal{E}$. Il y a donc dans $\mathcal{E}$, C_n^p sous-ensembles à $p+1$ éléments, contenant α.
Combien y a-t-il dans $\mathcal{E}$, de sous-ensembles à $p+1$ éléments, et ne contenant pas α ? Pour ces sous-ensembles là, puisqu'ils ne contiennent pas α, il faut choisir leurs $p+1$ éléments parmi les n éléments de $\mathcal{E}$ différents de α. Il y a donc C_n^{p+1} sous-ensembles de ce type. D'où le résultat : $C_{n+1}^{p+1} = C_n^p + C_n^{p+1}$.

Cette proposition est d'un grand intérêt pour le calcul des coefficients C_n^p. Après avoir remarqué que, pour tout $n \in \mathbb{N}$, $C_n^0 = 1$ et $C_n^n = 1$, car il n'y a, dans un ensemble à n éléments, qu'un seul sous-ensemble à 0 élément : l'ensemble vide, et qu'un seul sous-ensemble à n éléments : l'ensemble lui-même, on peut obtenir de façon mécanique les « premiers » coefficients C_n^p. Ce procédé est connu sous le nom de : triangle (voir la disposition des tableaux) de Pascal.
Pour remplir, par exemple, le tableau suivant :

$$\begin{array}{ccccc} C_0^0 & & & & \\ C_1^0 & C_1^1 & & & \\ C_2^0 & C_2^1 & C_2^2 & & \\ C_3^0 & C_3^1 & C_3^2 & C_3^3 & \\ C_4^0 & C_4^1 & C_4^2 & C_4^3 & C_4^4 \end{array}$$

Il suffit de faire fonctionner l'algorithme :

$$\begin{array}{ccc} C_n^p & \overset{+}{\rightarrow} & C_n^{p+1} \\ & & \downarrow = \\ & & C_{n+1}^{p+1} \end{array}$$

On obtient alors :

$$\begin{array}{ccccc} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ 1 & 4 & 6 & 4 & 1 \end{array}$$

1.3.4 Binôme de Newton

Théorème 1.3.5 (Formule du binôme) *Soient a et b des nombres réels. Soit $n \in \mathbb{N}$.*

$$(a+b)^n = \sum_{p=0}^{n} C_n^p a^{n-p} b^p$$

Démonstration 1.3.5 Démontrons la formule [15], par récurrence sur l'exposant figurant dans le membre de gauche. Si l'exposant est zéro, alors la formule est vraie, car :

$$(a+b)^0 = 1 = C_0^0 a^0 b^0 = \sum_{p=0}^{0} C_0^p a^{0-p} b^p.$$

14. La notation $\forall$ signifie : pour tout. $\exists$ signifie : il existe.
15. $\sum$ est la notation usuelle de la somme. $\sum_{p=0}^{n} u_p = u_0 + u_1 + \cdots + u_{n-1} + u_n$.

Supposons la formule démontrée pour l'entier n. Alors :

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{p=0}^{n} C_n^p a^{n-p}b^p \\
&= \sum_{p=0}^{n} C_n^p a^{n+1-p}b^p + \sum_{p=0}^{n} C_n^p a^{n-p}b^{p+1} \\
&= \sum_{p=0}^{n} C_n^p a^{n+1-p}b^p + \sum_{p=0}^{n} C_n^p a^{n+1-(p+1)}b^{p+1} \\
&= \sum_{p=0}^{n} C_n^p a^{n+1-p}b^p + \sum_{p=1}^{n+1} C_n^{p-1} a^{n+1-p}b^p \\
&= C_n^0 a^{n+1} + \sum_{p=1}^{n} \left(C_n^{p-1} + C_n^p\right) a^{n+1-p}b^p + C_n^n b^{n+1} \\
&= C_{n+1}^0 a^{n+1} + \sum_{p=1}^{n} C_{n+1}^p a^{n+1-p}b^p + C_{n+1}^{n+1} b^{n+1} \\
&= \sum_{p=0}^{n+1} C_{n+1}^p a^{n+1-p}b^p
\end{aligned}$$

La formule est vraie pour l'exposant $n+1$. Donc la formule est vraie pour tout $n \in \mathbb{N}$.

Exercice 1.3.3 *Montrer que $\sum_{p=0}^{n} C_n^p = 2^n$. En déduire le nombre total de sous-ensembles dans un ensemble à n éléments.*

Exercice 1.3.4 *Soit $\mathcal{E}$ un ensemble à n éléments ($n \in \mathbb{N}$). Combien y a-t-il de bijections de $\mathcal{E}$ dans lui-même ?*

Chapitre 2

Nombres complexes

2.1 L'ensemble $\mathbb{C}$ des nombres complexes

2.1.1 Une construction de $\mathbb{C}$

Une équation sans solution dans $\mathbb{R}$

Dans $\mathbb{N}$, l'équation d'inconnue n : $n+1=0$, n'a pas de solution. Or, fabriquer une solution pour cette équation permet de franchir une étape importante dans la science mathématique. Cette étape conduit de $\mathbb{N}$ à $\mathbb{Z}$, de la numération à l'algèbre. De même, dans $\mathbb{R}$, l'équation d'inconnue x : $x^2+1=0$, n'a pas de solution. En fabriquer une, conduit à introduire un nombre non réel dans l'univers des nombres.
Comment fabriquer une telle solution ? Une méthode consiste à considérer l'injection f de $\mathbb{R}$ dans $\mathbb{R}^2$ (l'ensemble des couples de nombres réels) définie par : $x \mapsto (x,0)$, et à munir $\mathbb{R}^2$ de deux lois internes : $\bullet$ et $*$, qui prolongent [1] les lois $+$ et $\times$ définies sur $\mathbb{R}$ et telles qu'il existe un couple dont le carré soit égal au couple $(-1,0)$.

Une injection de $\mathbb{R}$ dans $\mathbb{R}^2$

On considère l'application f de $\mathbb{R}$ dans $\mathbb{R}^2$, définie par : $f(x)=(x,0)$.

Exercice 2.1.1 *Montrer que l'application f définie ci-dessus est injective.*

Une addition sur $\mathbb{R}^2$

Cette loi interne sera notée $\bullet$.
Sur $\mathbb{R}^2$, on dispose d'une addition "naturelle" composante par composante. On définit donc la somme de deux couples de la manière suivante :

$$(x,y)\bullet(x',y')=(x+x',y+y')$$

On vérifie facilement que la somme ainsi définie, possède les propriétés suivantes [2] :

1. Associativité et commutativité héritées de la somme dans $\mathbb{R}$.
2. $(0,0)$ est l'élément neutre.
3. Tout couple (x,y) possède un opposé : $(-x,-y)$.

Exercice 2.1.2 *Vérifier que la somme ainsi définie prolonge la somme des nombres réels.*

Une multiplication sur $\mathbb{R}^2$

Cette loi interne sera notée $*$.
Il n'y a pas de multiplication "naturelle" sur $\mathbb{R}^2$. On peut penser, par exemple, en interprétant les éléments de $\mathbb{R}^2$ comme les coordonnées des vecteurs du plan, au produit scalaire pour tenter de définir une multiplication sur $\mathbb{R}^2$. Or, le produit scalaire ne fournit pas de loi interne car le produit scalaire de deux vecteurs est un nombre réel. Autrement dit : on sort de $\mathbb{R}^2$ lorsqu'on calcule un produit scalaire à l'aide des coordonnées.

1. « Prolongent » signifie :
$(\forall x\in\mathbb{R})(\forall y\in\mathbb{R}) \quad f(x+y)=f(x)\bullet f(y)$
$(\forall x\in\mathbb{R})(\forall y\in\mathbb{R}) \quad f(x\times y)=f(x)*f(y)$

2. Structure de groupe abélien.

La définition du produit ne peut être aussi simple que la définition de la somme [3].
On adopte la définition suivante pour le produit (la multiplication) :

$$(x, y) * (x', y') = (xx' - yy', xy' + x'y)$$

Exercice 2.1.3 *Montrer que le produit ainsi défini prolonge le produit des nombres réels.*

On vérifie que ce produit possède les propriétés suivantes:

1. Associativité et commutativité.
2. $(1, 0)$ est l'élément neutre.
3. Tout couple de nombres réels : (x, y), différent de $(0, 0)$, possède un inverse :

$$\left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}\right)$$

.

4. Distributivité par rapport l'addition.

Exercice 2.1.4 *Calculer* $(0, 1) * (0, 1)$.

Une construction de $\mathbb{C}$

Tout est maintenant en place pour définir les nombres complexes. Le passage de $\mathbb{R}^2$ à $\mathbb{C}$ s'effectue par un simple jeu de notations.

Définition et notation 2.1.1 $\mathbb{R}^2$ *muni des lois* $*$ *et* $\bullet$ *définies ci-dessus est noté :* $\mathbb{C}$. $\mathbb{C}$ *est l'ensemble des nombres complexes. Le couple* (x, y) *de* $\mathbb{R}^2$ *est noté* [4] $x + iy$ *lorsqu'il est considéré comme élément de* $\mathbb{C}$.

L'ensemble $\mathbb{C}$ est donc l'ensemble des nombres qui s'écrivent $x + iy$, avec $x \in \mathbb{R}$ et $y \in \mathbb{R}$.

Théorème 2.1.1 *Pour tout* x, *tout* y, *tout* x' *et tout* y' *dans* $\mathbb{R}$ *:*
$x + iy = x' + iy'$ *si et seulement si* $x = x'$ *et* $y = y'$.

Démonstration 2.1.1 Le théorème n'est qu'une conséquence immédiate de la définition de $x + iy$, car $(x, y) = (x', y')$ si et seulement si $x = x'$ et $y = y'$.

Simplifications d'écriture :

La somme $(x, y) \bullet (x', y')$ s'écrit $(x + iy) + (x' + iy')$.

Le produit $(x, y) * (x', y')$ s'écrit $(x + iy) \times (x' + iy')$, ou bien encore plus simplement $(x + iy)(x' + iy')$.

On retrouve donc dans $\mathbb{C}$ les notations usuelles adoptées dans $\mathbb{R}$ pour le produit et la somme [5]. L'utilisation des exposants sera donc étendue aux éléments de $\mathbb{C}$ pour obtenir des expressions de produits simplifiées.
On utilise également les notations simplifiées suivantes :

x au lieu de $x + i0$

iy au lieu de $0 + iy$

i au lieu de $0 + i1$

$2i$ plutôt que $i2$, mais $i\sqrt{2}$

$-iy$ plutôt que $i(-y)$

La soustraction et la division sont définies sur $\mathbb{C}$ comme sur $\mathbb{R}$:

soustraire z, c'est additionner l'opposé de z

diviser [6] par z, c'est multiplier par l'inverse de z.

3. Si on pose $(x, y) * (x', y') = (xx', yy')$, il n'existe alors aucun couple (x, y) tel que $(x, y) * (x, y) = (-1, 0)$.
4. En sciences physiques, la notation usuelle de i est : j.
5. $\mathbb{C}$ et $\mathbb{R}$ sont, muni de ces deux lois internes, deux exemples de corps.
6. "z divisé par z'" s'écrit $\frac{z}{z'}$ ou zz'^{-1}.

2.1.2 Les nombres complexes

Nous avons réalisé notre objectif : construire une solution pour l'équation $x^2 + 1 = 0$ (voir le théorème 2.1.2). L'ensemble dans lequel cette solution a été obtenue n'est pas totalement étranger à $\mathbb{R}$ car $\mathbb{R}$ est « inclus » dans $\mathbb{C}$; ou pour être plus précis : $f(\mathbb{R}) \subset \mathbb{C}$, et comme f est injective, on ne s'efforce pas dans la pratique de distinguer $f(\mathbb{R})$ de $\mathbb{R}$. Les nombres réels peuvent ainsi être considérés comme des nombres complexes particuliers : ceux de type $x + i0$, avec $x \in \mathbb{R}$.

Définition et notation 2.1.2 *La notation $\mathbb{C}^*$ désigne l'ensemble $\mathbb{C} \setminus \{0\}$, c'est à dire : $\mathbb{C}$ privé de l'élément 0.*

Exercice 2.1.5 *Montrer que $\mathbb{C}^*$ est l'ensemble des éléments de $\mathbb{C}$ ayant un inverse [7] pour la loi $\times$.*

Théorème 2.1.2

$$i^2 = -1$$

Démonstration 2.1.2 La démonstration est laissée en exercice. C'est une conséquence triviale de la définition de la multiplication.

Exercice 2.1.6 *Vérifier, pour tout x, tout y, tout x' et tout y' dans $\mathbb{R}$, les égalités suivantes [8] :*

1. $(x + iy) + (x' + iy') = (x + x') + i(y + y')$
2. $(x + iy)(x' + iy') = (xx' - yy') + i(xy' + x'y)$
3. $(x + iy)^{-1} = \frac{x}{x^2+y^2} - i\frac{y}{x^2+y^2}$

Forme algébrique

On utilise souvent une seule lettre : z, pour désigner un nombre complexe.

Définition 2.1.3 (Forme algébrique) *Soit $z \in \mathbb{C}$. On dit que $x+iy$ est la forme algébrique de z si $z = x+iy$, $x \in \mathbb{R}$ et $y \in \mathbb{R}$.*

Exemple $1 + i$ est la forme algébrique d'un élément de $\mathbb{C}$.
Exemple $1 + (1 + i)$ n'est pas une forme algébrique, car ce n'est pas de la forme « $x + iy$ », avec $x \in \mathbb{R}$ et $y \in \mathbb{R}$.

Définition et notation 2.1.4 (Partie réelle) *Si $x + iy$ est la forme algébrique de nombre complexe z, alors le nombre réel x est la partie réelle du nombre complexe z et on écrit : $x = \Re e(z)$.*

Définition et notation 2.1.5 (Partie imaginaire) *Si $x + iy$ est la forme algébrique de nombre complexe z, alors le nombre réel y est la partie imaginaire du nombre complexe z et on écrit : $y = \Im m(z)$.*

Conjugué

Définition et notation 2.1.6 (Conjugué) *Soit $x+iy$ la forme algébrique du nombre complexe z. On appelle conjugué de z le nombre $x - iy$. Le conjugué de z se note $\bar{z}$. On dit que les nombres complexes z et z' sont conjugués lorsque $\bar{z'} = z$.*

Exercice 2.1.7 *Montrer que [9] :*

1. *Pour tout z et tout z' dans $\mathbb{C}$: $z = \bar{z'} \iff z' = \bar{z}$.*
2. *Pour tout $z \in \mathbb{C}$, $\bar{\bar{z}} = z$.*
3. *Si $x + iy$ est la forme algébrique de z, alors $z\bar{z} = x^2 + y^2$.*

Exercice 2.1.8 *Montrer que $\Re e(z) = \frac{z+\bar{z}}{2}$ et $\Im m(z) = \frac{z-\bar{z}}{2i}$.*

7. On dit aussi : "éléments inversibles".

8. Pour cet exercice, il faut faire « fonctionner les définitions ». Dans la pratique, il est bien évident qu'on ne passe pas par les couples de nombres réels pour effectuer des calculs sur les nombres complexes ; bien au contraire, on utilise directement les règles de calculs exposées dans cet exercice.

9. « $\iff$ » signifie : « si et seulement si ». C'est le symbole de l'équivalence. « $\Rightarrow$ » signifie : « implique » ou « a pour conséquence ».

Affixe

Considérons le plan muni du repère orthonormé $(O, \overrightarrow{u}, \overrightarrow{v})$. Tout point du plan possède alors des coordonnées, et tout vecteur se décompose dans la base $(\overrightarrow{u}, \overrightarrow{v})$.

Définition 2.1.7 (Affixe d'un point) *On dit que le point M, de coordonnées (x, y), a pour affixe le nombre complexe z lorsque $z = x + iy$.*

On peut donc établir une bijection entre l'ensemble des nombres complexes et l'ensemble des points du plan, dès que le plan est muni d'un repère. Le point d'affixe z est l'image de z par cette bijection. Ceci permet de représenter les nombres complexes à l'aide de points, de « faire un dessin ».

Définition 2.1.8 (Affixe d'un vecteur) *Considérons le vecteur $\overrightarrow{w}$ tel que $\overrightarrow{w} = x\overrightarrow{u} + y\overrightarrow{v}$. Le nombre complexe $z = x + iy$ est alors l'affixe de $\overrightarrow{w}$.*

Forme trigonométrique

Définition et notation 2.1.9 (Module) *Soit $x + iy$ la forme algébrique du nombre complexe z. Le nombre réel positif $\sqrt{x^2 + y^2}$ est alors le module du nombre complexe z. $|z|$ désigne le module de z.*

Exercice 2.1.9 *Rédiger les démonstrations de :*

1. $z = 0 \iff |z| = 0$
2. $(\forall z \in \mathbb{C}^*) \quad |\frac{1}{z}| = \frac{1}{|z|}$
3. $(\forall z \in \mathbb{C}^*) \quad \frac{1}{z} = \frac{\overline{z}}{|z|^2}$
4. $(\forall (z, z') \in \mathbb{C}^2) \quad |zz'| = |z||z'|$

La notation employée pour le module d'un nombre complexe est identique à celle employée pour la valeur absolue d'un nombre réel. Ceci est parfaitement légitime car pour tout x réel, vu comme nombre complexe dont la partie imaginaire est nulle, le calcul du module est : $\sqrt{x^2 + 0^2} = \sqrt{x^2}$, ce qui est bien égal à la valeur absolue de x.

Théorème 2.1.3 (Inégalité triangulaire)

$$(\forall z \in \mathbb{C})(\forall z' \in \mathbb{C}) \quad |z + z'| \leqslant |z| + |z'|$$

Démonstration 2.1.3 Si $z' = 0$ alors l'inégalité est triviale.
Supposons $z' \neq 0$. Notons $x + iy$ la forme algébrique de z et $x' + iy'$ celle de z'. Alors, pour tout $\lambda \in \mathbb{R}$ et tout $z \in \mathbb{C}$, l'expression : $(x'^2 + y'^2)\lambda^2 + 2(xx' + yy')\lambda + x^2 + y^2$ est un trinôme du second degré en λ. Or, ce trinôme est égal à $|z + \lambda z'|^2$; il est donc, pour tout $\lambda \in \mathbb{R}$ supérieur ou égal à 0. Par conséquent, son discriminant est inférieur ou égal à 0. Ceci s'écrit : $4(xx' + yy)^2 - 4(x^2 + y^2)(x'^2 + y'^2) \leqslant 0$, ou bien encore : $(xx' + yy')^2 \leqslant (x^2 + y^2)(x'^2 + y'^2)$. On en déduit :

$$\begin{aligned} |z + z'|^2 &= x^2 + y^2 + 2(xx' + yy') + x'^2 + y'^2 \\ &\leqslant x^2 + y^2 + 2\sqrt{x^2 + y^2}\,\sqrt{x'^2 + y'^2} + x'^2 + y'^2 \\ &= (|z| + |z'|)^2 \end{aligned}$$

D'où $|z + z'| \leqslant |z| + |z'|$.

On remarque [10] que $|z| = OM = \|\overrightarrow{w}\|$, lorsque M et $\overrightarrow{w}$ ont pour affixe z.
Si $|z| = 1$, alors le point M d'affixe z est un point du cercle de centre l'origine et de rayon 1 : le cercle trigonométrique. Dans ce cas, si t est une mesure en radians de $\left(\overrightarrow{u}, \overrightarrow{OM}\right)$, les coordonnées de M sont $(\cos t, \sin t)$. Notons que pour tout $z \in \mathbb{C}^*$, $\frac{z}{|z|}$ est de module 1.

Définition et notation 2.1.10 (Argument) *Soit z un nombre complexe différent de 0. Tout nombre réel t tel que $\frac{z}{|z|} = \cos t + i \sin t$ est un argument de z. La notation usuelle du nombre complexe $\cos t + i \sin t$ est : e^{it} (lire : "exponentielle it").*

10. On rappelle que $\|\overrightarrow{w}\|$ est la norme de $\overrightarrow{w}$.

Un nombre complexe est donc entièrement déterminé par son module et un de ses arguments. Si z a pour module r et pour argument t, alors $\Re e(z) = r\cos t$ et $\Im m(z) = r\sin t$.

Définition 2.1.11 (Forme trigonométrique) *Soit z un nombre complexe non nul de module r et d'argument t. On a : $z = re^{it}$. On dit alors que re^{it} est la forme trigonométrique de z.*

Exercice 2.1.10 *Montrer que :*
$(\forall r \in]0,+\infty[)\,(\forall r' \in]0,+\infty[)\,(\forall t \in \mathbb{R})(\forall t' \in \mathbb{R})$
$re^{it} = r'e^{it'} \iff (r = r' \text{ et } (\exists k \in \mathbb{Z}) \quad t = t' + 2\pi k)$

Exercice 2.1.11 *Soit $(\alpha, \beta) \in \mathbb{R}^2$. On rappelle les formules trigonométriques suivantes :*

$$\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$$
$$\sin(\alpha+\beta) = \cos\alpha\sin\beta + \sin\alpha\cos\beta$$

Les formes trigonométriques respectives des nombres z et z' étant re^{it} et $r'e^{it'}$, montrer que :

1. $\bar{z} = re^{-it}$
2. $\frac{1}{z} = \frac{1}{r}e^{-it}$
3. $zz' = rr'e^{i(t+t')}$
4. $\frac{z}{z'} = \frac{r}{r'}e^{i(t-t')}$

Deux conséquences des résultats de l'exercice 2.1.11 sont les formules de Moivre et d'Euler.

Formule de Moivre

$$(\forall \theta \in \mathbb{R})(\forall n \in \mathbb{Z}) \quad (\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$$

Ce qui s'écrit, en utilisant la notation exponentielle :

$$(\forall \theta \in \mathbb{R})(\forall n \in \mathbb{Z}) \quad \left(e^{i\theta}\right)^n = e^{in\theta}$$

Démonstration 2.1.3 On se ramène au cas $n \geqslant 0$, car si $n < 0$, alors $n = -m$, avec $m \in \mathbb{N}$, et [11] $\left(e^{i\theta}\right)^n = \left(e^{i\theta}\right)^{-m} = \left(e^{i(-\theta)}\right)^m$. Montrons donc, par récurrence sur l'entier naturel n, la validité de la formule de Moivre.
Pour $n = 0$, comme $z^0 = 1$ quel que soit $z \in \mathbb{C}$, $\cos 0 = 1$ et $\sin 0 = 0$, la formule de Moivre est vérifiée.
Supposons l'égalité $\left(e^{i\theta}\right)^n = e^{in\theta}$ vraie.
Montrons qu'alors $\left(e^{i\theta}\right)^{n+1} = e^{i(n+1)\theta}$ est vraie.
Par définition : $\left(e^{i\theta}\right)^{n+1} = \left(e^{i\theta}\right)^n e^{i\theta}$.
D'où, en utilisant l'hypothèse de récurrence :

$$\begin{aligned}\left(e^{i\theta}\right)^{n+1} = e^{in\theta}e^{i\theta} &= (\cos n\theta + i\sin n\theta)(\cos\theta + i\sin\theta)\\ &= \cos n\theta\cos\theta - \sin n\theta\sin\theta + i(\sin n\theta\cos\theta + \cos n\theta\sin\theta)\\ &= \cos(n\theta+\theta) + i\sin(n\theta+\theta)\\ &= \cos((n+1)\theta) + i\sin((n+1)\theta) = e^{i(n+1)\theta}\end{aligned}$$

Si la formule est vraie pour l'entier n, elle l'est pour $n+1$, donc pour tout $n \in \mathbb{N}$.

Formules d'Euler

$$(\forall \theta \in \mathbb{R}) \quad \begin{cases}\cos\theta = \dfrac{e^{i\theta} + e^{-i\theta}}{2}\\ \sin\theta = \dfrac{e^{i\theta} - e^{-i\theta}}{2i}\end{cases}$$

11. Le résultat $\frac{1}{e^{it}} = e^{-it}$ est utilisé ici.

Exemple d'utilisation des formules de Moivre et d'Euler

Calculer $\int_0^{\frac{\pi}{2}} \cos^3 t\, dt$ commence [12] par la recherche d'un primitive de $t \mapsto \cos^3 t$. Il faut donc nous débarrasser des produits, des exposants ; c'est ce qu'on appelle : linéariser $\cos^3 t$. Pour ce faire, utilisons la formule d'Euler : $\cos t = \frac{e^{it}+e^{-it}}{2}$. Comme $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$, on obtient :

$$\begin{aligned}\cos^3 t &= \frac{1}{8}(e^{it} + e^{-it})^3 \\ &= \frac{1}{8}((e^{it})^3 + 3(e^{it})^2 e^{-it} + 3e^{it}(e^{-it})^2 + (e^{-it})^3)\end{aligned}$$

En utilisant les formules de Moivre, puis d'Euler, on obtient :

$$\begin{aligned}(e^{it})^3 + 3(e^{it})^2 e^{-it} + 3e^{it}(e^{-it})^2 + (e^{-it})^3 &= e^{3it} + 3e^{2it}e^{-it} + 3e^{it}e^{-2it} + e^{-3it} \\ &= e^{3it} + 3e^{it} + 3e^{-it} + e^{-3it} \\ &= 2\left(\frac{e^{3it} + e^{-3it}}{2}\right) + 6\left(\frac{e^{it} + e^{-it}}{2}\right) \\ &= 2\cos 3t + 6\cos t\end{aligned}$$

D'où :

$$\begin{aligned}\int_0^{\frac{\pi}{2}} \cos^3 t\, dt &= \int_0^{\frac{\pi}{2}} \frac{1}{4}\cos 3t + \frac{3}{4}\cos t\, dt \\ &= \left[\frac{1}{12}\sin 3t + \frac{3}{4}\sin t\right]_0^{\frac{\pi}{2}} \\ &= \frac{1}{12}\sin\frac{3\pi}{2} + \frac{3}{4}\sin\frac{\pi}{2} - 0 \\ &= -\frac{1}{12} + \frac{3}{4} \\ &= \frac{2}{3}\end{aligned}$$

Exercice 2.1.12 *Calculer :*

$$\int_0^{\pi} \sin^2 t \cos t\, dt$$

2.2 Équations du second degré

2.2.1 Équations de type $z^2 = \alpha$

Nous savons que dans $\mathbb{R}$, une équation de type : $x^2 = a$, n'a pas de solution quand le nombre réel a est strictement négatif. La construction de $\mathbb{C}$ a permis d'obtenir une solution pour l'équation $x^2 = -1$. Ceci a pour conséquence la proposition suivante :

Proposition 2.2.1 *Pour tout nombre réel a, l'équation d'inconnue z : $z^2 = a$, a pour ensemble des solutions dans $\mathbb{C}$:*

1. $\left\{i\sqrt{|a|}\,,\, -i\sqrt{|a|}\right\}$, *si* $a < 0$.
2. $\{\sqrt{a}\,,\, -\sqrt{a}\}$, *si* $a > 0$.
3. $\{0\}$, *si* $a = 0$.

Démonstration 2.2.1 La démonstration est laissée en exercice.

Proposition 2.2.2 *Soit α un nombre complexe différent [13] de 0.*
L'équation d'inconnue z : $z^2 = \alpha$, admet dans $\mathbb{C}$ deux solutions distinctes.

12. Le point de vue envisagé ici n'est pas celui d'un utilisateur de ces fameuses calculatrices "magiques" qui affichent un résultat qu'on ne comprend pas...

13. Notons que le cas $\alpha = 0$ a déjà été envisagé dans la proposition 2.2.1.

Démonstration 2.2.2 0 n'est pas solution de l'équation. Soit $z \in \mathbb{C}^*$. Considérons les formes trigonométriques de α et de z : $\rho e^{i\theta} = \alpha$ et $re^{it} = z$. Alors, on a :

$$z^2 = \alpha \iff \left(re^{it}\right)^2 = \rho e^{i\theta} \iff r^2 e^{2it} = \rho e^{i\theta}$$

Or, cette dernière égalité équivaut à : $r^2 = \rho$ et $2t = \theta + 2\pi k$, pour un certain k dans $\mathbb{Z}$. On en déduit : $r = \sqrt{\rho}$ et $t = \frac{\theta}{2} + k\pi$. Les solutions de l'équation $z^2 = \alpha$ sont donc les nombres dont la forme trigonométrique est : $\sqrt{\rho}\, e^{i\left(\frac{\theta}{2}+k\pi\right)}$. Or, $e^{i\left(\frac{\theta}{2}+k\pi\right)} = e^{i\frac{\theta}{2}}$, si k est pair, et $e^{i\left(\frac{\theta}{2}+k\pi\right)} = e^{i\left(\frac{\theta}{2}+\pi\right)} = -e^{i\frac{\theta}{2}}$, si k est impair. D'où, les solutions de $z^2 = \alpha$ sont $\sqrt{\rho}\, e^{i\frac{\theta}{2}}$ et $-\sqrt{\rho}\, e^{i\frac{\theta}{2}}$.

Pour $a \in \mathbb{R}^+$, $\sqrt{a}$ désigne "le nombre positif dont le carré vaut a". Pour α quelconque dans $\mathbb{C}$, il est moins aisé de donner une définition de la notation $\sqrt{\alpha}$. On pourrait, par exemple, décider que $\sqrt{\alpha}$ est le nombre complexe ayant un argument dans $[0,\pi[$, et dont le carré vaut α. Mais, comme une telle définition ne se rencontre pas dans les livres de mathématiques, nous éviterons de parler de la racine carrée de α, d'écrire $\sqrt{\alpha}$, lorsqu'α n'est pas un nombre réel positif. On pourrait cependant employer l'expression : « les racines carrées de α » pour désigner les nombres complexes dont le carré est α.

Pour toute équation de type $z^2 = \alpha$, lorsque que la forme triginométrique de α n'est pas donnée, il est judicieux de poser le problème de la recherche des solutions de la manière suivante :
Soit $a + ib$ la forme algébrique de α ;

1. On pose $z = x + iy$ afin de déterminer les valeurs réelles x et y telles que $z^2 = \alpha$;
2. L'équation $z^2 = \alpha$ s'écrit alors : $x^2 - y^2 + 2ixy = a + ib$ et est équivalente au système : $\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$;
3. Si $z^2 = \alpha$ alors $|z|^2 = |\alpha|$ et donc : $x^2 + y^2 = \sqrt{a^2 + b^2}$;
4. On résout le système : $\begin{cases} x^2 - y^2 = a \\ x^2 + y^2 = \sqrt{a^2 + b^2} \end{cases}$;
5. Les nombres x et y solutions de ce dernier système et dont le produit xy est de même signe que b sont les nombres cherchés.

2.2.2 Équations de type $az^2 + bz + c = 0$, $a \neq 0$

Définition 2.2.1 (Trinôme du second degré) *Soient b et c dans $\mathbb{C}$, et a dans $\mathbb{C}^*$.*

$$az^2 + bz + c$$

est un trinôme du second degré en z.

Définition et notation 2.2.2 (Discriminant) *Soient b et c dans $\mathbb{C}$, et a dans $\mathbb{C}^*$. Le discriminant du trinôme $az^2 + bz + c$, se note Δ et vaut : $b^2 - 4ac$.*

Théorème 2.2.3 *Soient b et c des nombres complexes quelconques, et a un nombre complexe différent de 0. Soit Δ le discriminant du trinôme $az^2 + bz + c$. Soit δ dans $\mathbb{C}$ tel que $\delta^2 = \Delta$. Alors, les solutions dans $\mathbb{C}$ de l'équation du second degré $az^2 + bz + c = 0$ sont : $\dfrac{-b+\delta}{2a}$ et $\dfrac{-b-\delta}{2a}$.*

Démonstration 2.2.3

$$\begin{aligned} az^2 + bz + c &= a\left(z^2 + \frac{b}{a}z + \frac{c}{a}\right) = a\left[\left(z + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right] \\ &= a\left[\left(z + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right] = a\left[\left(z + \frac{b}{2a}\right)^2 - \left(\frac{\delta}{2a}\right)^2\right] \\ &= a\left(z + \frac{b}{2a} + \frac{\delta}{2a}\right)\left(z + \frac{b}{2a} - \frac{\delta}{2a}\right) \\ &= a\left(z - \frac{-b-\delta}{2a}\right)\left(z - \frac{-b+\delta}{2a}\right) \end{aligned}$$

D'où, $az^2 + bz + c = 0 \iff \begin{cases} z = \frac{-b+\delta}{2a} \\ \text{ou} \\ z = \frac{-b-\delta}{2a} \end{cases}$

Définition 2.2.3 (Racines) *On considère le trinôme az^2+bz+c. Les solutions de l'équation $az^2+bz+c=0$ s'appellent les racines du trinôme az^2+bz+c.*

Définition 2.2.4 (Racine double) *On considère le trinôme az^2+bz+c. Lorsque l'équation $az^2+bz+c=0$ admet une unique solution, cette solution est la racine double du trinôme az^2+bz+c.*

Exercice 2.2.1 *Soit $P(z)=az^2+bz+c$ un trinôme du second degré en z. Montrer que la somme des racines de $P(z)$ vaut $\frac{-b}{a}$; montrer que le produit des racines de $P(z)$ vaut $\frac{c}{a}$.*

Exercice 2.2.2 *Montrer que si les coefficients a, b et c sont réels, et si le discriminant du trinôme az^2+bz+c est un nombre réel strictement négatif, alors les solutions de l'équation $az^2+bz+c=0$ sont des nombres complexes conjugués.*

2.3 Racines n-ièmes de l'unité

Théorème 2.3.1 *Soit n un élément de $\mathbb{N}\setminus\{0\}$.*
Les n solutions dans $\mathbb{C}$ de l'équation $z^n=1$, sont les nombres : $e^{\frac{2\pi ki}{n}}$, $k\in[\![0,n-1]\!]$.

Définition 2.3.1 (Racines n-ièmes de l'unité) *Les n solutions de $z^n=1$ s'appellent les racines n-ièmes de l'unité.*

Lemme 2.3.1.1 *Soit k un nombre entier relatif quelconque, et n un nombre entier naturel non nul.*
Il existe un unique couple (q,r) d'éléments de $\mathbb{Z}$ tel que :
$k=nq+r$ et $r\in[\![0,n-1]\!]$.

Lemme 2.3.1.2 *Soit $n\in\mathbb{N}\setminus\{0\}$.*
L'application $f:[\![0,n-1]\!]\to\mathbb{C}$ définie par $f(r)=e^{\frac{2\pi ri}{n}}$ est injective.

Démonstration 2.3.1 Admettons, pour l'instant, les lemmes 2.3.1.1 et 2.3.1.2, et démontrons le théorème.
0 n'est pas solution de l'équation. Soit $z\in\mathbb{C}^*$. Soit re^{it} la forme trigonométrique de z.

$$\begin{aligned}
z^n=1 &\iff \left(re^{it}\right)^n=1\\
&\iff r^ne^{int}=1e^{0i}\\
&\iff \begin{cases} & r^n=1\\ (\exists k\in\mathbb{Z}) & nt=2\pi k\end{cases}\\
&\iff \begin{cases} & r=1\\ (\exists k\in\mathbb{Z}) & t=\frac{2\pi k}{n}\end{cases}
\end{aligned}$$

Les solutions de l'équation $z^n=1$ sont donc les nombres de la forme : $e^{\frac{2\pi ki}{n}}$, avec $k\in\mathbb{Z}$. Montrons que l'ensemble des nombres $e^{\frac{2\pi ki}{n}}$, avec $k\in\mathbb{Z}$, est égal l'ensemble des nombres $e^{\frac{2\pi ri}{n}}$, avec $r\in[\![0,n-1]\!]$. Soit $k\in\mathbb{Z}$. D'après le lemme 2.3.1.1, il existe un unique couple d'entiers (q,r), tel que $k=nq+r$ et $r\in[\![0,n-1]\!]$. Alors,

$$\begin{aligned}
e^{\frac{2\pi ki}{n}} &= e^{\frac{2\pi(nq+r)i}{n}}=e^{2\pi qi+\frac{2\pi ri}{n}}\\
&= e^{2\pi qi}e^{\frac{2\pi ri}{n}}=1e^{\frac{2\pi ri}{n}}\\
&= e^{\frac{2\pi ri}{n}}
\end{aligned}$$

Il y a donc autant de nombres $e^{\frac{2\pi ki}{n}}$ que de nombres $e^{\frac{2\pi ri}{n}}$ avec $r\in[\![0,n-1]\!]$. Or, d'après le lemme 2.3.1.2, il y a autant de nombres $e^{\frac{2\pi ri}{n}}$ avec $r\in[\![0,n-1]\!]$ que de nombres dans $[\![0,n-1]\!]$ qui est un ensemble à n éléments. L'équation $z^n=1$ a donc exactement n solutions, et ces solutions sont les nombres $e^{\frac{2\pi ki}{n}}$ avec $k\in[\![0,n-1]\!]$.

Démonstration 2.3.1.2 Démonstration du lemme 2.3.1.1 :
Comme $\mathbb{R}=\bigcup_{q\in\mathbb{Z}}[nq,n(q+1)[$ et que les intervalles $[nq,n(q+1)[$ sont deux à deux disjoints, on en déduit que, pour tout $k\in\mathbb{Z}$, il existe un unique $q\in\mathbb{Z}$ tel que : $k\in[nq,n(q+1)[$. Mais alors $k-nq=r\in[\![0,n-1]\!]$, et comme q est déterminé de façon unique, r l'est aussi.

Démonstration 2.3.1.2 Démonstration du lemme 2.3.1.2 :
Si r et r' sont deux nombres entiers de l'intervalle $[0, n[$, on a :

$$\begin{aligned} f(r) = f(r') &\iff e^{\frac{2\pi r i}{n}} = e^{\frac{2\pi r' i}{n}} \\ &\iff (\exists m \in \mathbb{Z}) \quad \frac{2\pi r}{n} = \frac{2\pi r'}{n} + 2\pi m \\ &\iff (\exists m \in \mathbb{Z}) \quad r = r' + nm \end{aligned}$$

Puisque $r' \in [0, n[$, on a, d'après cette dernière égalité : $r \in [nm, n(m+1)[$. Comme $r \in [0, n[$, on en déduit $m = 0$ et donc $r = r'$.

Exercice 2.3.1 *Résoudre dans $\mathbb{C}$ l'équation $z^3 = -1$.*

Exercice 2.3.2 *Soit $n \in \mathbb{N} \setminus \{0, 1\}$. Soit α une des $n-1$ racines n-ièmes de l'unité différentes de 1. Calculer $1 + \alpha + \alpha^2 + \cdots + \alpha^{n-1}$.*

Chapitre 3

Polynômes

Dans ce chapitre, $\mathbb{K}$ désigne indifféremment $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

3.1 L'anneau $\mathbb{K}[X]$

3.1.1 L'ensemble $\mathbb{K}[X]$

Définition et notation 3.1.1 (Suite) *Une suite d'éléments de $\mathbb{K}$ est une application de $\mathbb{N}$ dans $\mathbb{K}$.*
Soit u une suite d'éléments de $\mathbb{K}$. On adopte la notation u_n à la place de la notation habituelle de l'image de n par l'application u : $u(n)$.
D'où cette autre façon de noter u : $(u_n)_{n\in\mathbb{N}}$.

Les suites arithmétiques ou géométriques étudiées au lycée, sont des exemples de suites de nombres réels.

Notation 3.1.2 *L'ensemble des suites d'éléments de $\mathbb{K}$ se note : $\mathbb{K}^{\mathbb{N}}$.*

Définition 3.1.3 (Termes) *Soit $u = (u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$. u_0, u_1, u_2,..., u_n,... sont les termes de u.*

Définition 3.1.4 (Rang) *Soit $u = (u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$. Soit $m \in \mathbb{N}$. Le terme de rang m de la suite u est : u_m.*

Définition 3.1.5 (Terme général) *Soit $u = (u_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{K}$. u_n est le terme général de u.*

Définition et notation 3.1.6 (Suite presque nulle) *Soit u une suite d'éléments de $\mathbb{K}$. On dit que u est une suite presque nulle, si $u_n = 0$ pour tout $n \in \mathbb{N} \setminus \mathcal{F}$, où $\mathcal{F}$ est un sous-ensemble fini de $\mathbb{N}$.*
L'ensemble des suites presque nulles d'éléments de $\mathbb{K}$ se note : $\mathbb{K}[X]$.

Définition 3.1.7 (Suite nulle à partir d'un certain rang) *On dit que la suite u d'éléments de $\mathbb{K}$ est nulle à partir d'un certain rang s'il existe $n_0 \in \mathbb{N}$ tel que $u_n = 0$ pour tout $n \in \mathbb{N} \cap [n_0 + 1, +\infty[$.*

Définition et notation 3.1.8 (Support) *Soit $u \in \mathbb{K}^{\mathbb{N}}$.*
$\mathrm{supp}(u)$, *le support de la suite u, est défini* [1] *par :* $\mathrm{supp}(u) = \{n \in \mathbb{N} \mid u_n \neq 0\}$.

Remarque : $\mathrm{supp}(u) = \emptyset \iff (\forall n \in \mathbb{N}) \quad u_n = 0$.

Définition 3.1.9 *La suite dont le terme général est nul s'appelle la suite nulle.*

Exercice 3.1.1 *Soit $u \in \mathbb{K}^{\mathbb{N}}$. Montrer que les trois affirmations suivantes sont équivalentes.*

1. *u est presque nulle.*
2. *u est nulle à partir d'un certain rang.*
3. *u est à support fini, c'est à dire :* $\mathrm{supp}(u)$ *est un ensemble fini.*

1. La suite de symboles $\{n \in \mathbb{N} \mid u_n \neq 0\}$ signifie : l'ensemble des nombres entiers naturels n tels que $u_n \neq 0$.

Définition et notation 3.1.10 (Degré) *Soit u une suite presque nulle d'éléments de $\mathbb{K}$. Le degré de u, noté* $\deg(u)$*, est défini par :*

$$\deg(u) = \begin{cases} \max(\mathrm{supp}(u)) & si\ \mathrm{supp}(u) \neq \emptyset \\ -\infty & si\ \mathrm{supp}(u) = \emptyset \end{cases}$$

Autrement [2] *dit : le degré de u est le plus grand des nombres entiers n tel que $u_n \neq 0$ si de tels nombres existent (*$\mathrm{supp}(u) \neq \emptyset$*), et si $u_n = 0$ pour tout n (*$\mathrm{supp}(u) = \emptyset$ *et donc u est la suite nulle), par convention, le degré de u est $-\infty$.*

Avoir posé le degré de la suite nulle égal à $-\infty$, nécessite de présenter les règles de calcul avec $-\infty$ qui seront utilisées.

- $(-\infty) + n = n + (-\infty) = -\infty$ pour tout n dans $\mathbb{N} \cup \{-\infty\}$.
- Tout nombre entier est strictement plus grand que $-\infty$.
- $\max\{-\infty, n\} = n$ pour tout n dans $\mathbb{N} \cup \{-\infty\}$.

3.1.2 Structures algébriques sur $\mathbb{K}[X]$

Nous allons, dans cette partie, définir une somme et un produit sur $\mathbb{K}[X]$ qui feront de $\mathbb{K}[X]$ ce qu'on appelle [3] un anneau commutatif.

Somme

Définition et notation 3.1.11 (Somme) *Soient $u = (u_n)_{n\in\mathbb{N}}$ et $v = (v_n)_{n\in\mathbb{N}}$ dans $\mathbb{K}^{\mathbb{N}}$.*
La somme de u et de v, notée $u + v$, est la suite dont le terme général est :

$$(u + v)_n = u_n + v_n$$

Remarque : Puisque $\mathbb{K}[X] \subset \mathbb{K}^{\mathbb{N}}$, la somme définie sur $\mathbb{K}^{\mathbb{N}}$ est définie de sur $\mathbb{K}[X]$. S'il est évident qu'une somme de suites est une suite, il est en revanche nécessaire de prouver qu'une somme de suites presque nulles est une suite presque nulle (voir l'exercice 3.1.2).

Exercice 3.1.2 *Démontrer que la somme ainsi définie sur $\mathbb{K}[X]$ possède les propriétés suivantes :*

1. *C'est une loi interne.*
2. *Elle est commutative.*
3. *Elle est associative.*
4. *Elle a pour élément neutre, la suite nulle.*
5. *Chaque suite $u = (u_n)_{n\in\mathbb{N}}$ admet un opposé, noté $-u$, de terme général $-u_n$.*

L'ensemble $\mathbb{K}[X]$ muni de cette somme est un groupe commutatif (on dit aussi : groupe abélien).

Théorème 3.1.1 *Pour tout u et tout v dans $\mathbb{K}[X]$:*

$$\deg(u + v) \leqslant \max\{\deg(u), \deg(v)\}$$

Démonstration 3.1.1 Soit $m = \max\{\deg(u), \deg(v)\}$. D'après la définition de la somme, $(u + v)_n = u_n + v_n$. Donc, si $n > m$, $(u + v)_n = 0$. D'où le théorème.

2. Pour un sous-ensemble non vide $\mathcal{E}$ de $\mathbb{R}$, la notation $\max \mathcal{E}$ désigne, s'il existe, le maximum de $\mathcal{E}$, c'est à dire : son plus grand élément.

3. Le nom de différentes structures algébriques sera donné à titre indicatif lorsque ces structures seront rencontrées dans le cours. Pour les amateurs de structures algébriques, la lecture des meilleures pages du volumineux [4] meublera utilement quelques longues soirées d'hiver... lorsqu'ils seront édudiants de second ou de troisième cycle. Ils trouveront dès à présent leur bonheur dans [5], déjà signalé en note page 5.

Produit

Définition et notation 3.1.12 (Produit) *Soient $u = (u_n)_{n\in\mathbb{N}}$ et $v = (v_n)_{n\in\mathbb{N}}$ dans $\mathbb{K}^{\mathbb{N}}$.*
Le produit de u par v est la suite, notée uv, dont le terme général[4] *est :*

$$(uv)_n = \sum_{k=0}^{n} u_{n-k}v_k = \sum_{i+j=n} u_i v_j$$

Définition et notation 3.1.13 (Symboles de Kronecker) *Les symboles de Kronecker : $\delta_{i\,j}$, sont définis pour tout i et tout j dans $\mathbb{N}$ par :*

$$\delta_{i\,j} = \begin{cases} 0 & si\ i \neq j \\ 1 & si\ i = j \end{cases}$$

Exercice 3.1.3 *Démontrer que le produit ainsi défini sur $\mathbb{K}[X]$ possède les propriétés suivantes :*

1. *C'est une loi interne.*
2. *Il est commutatif.*
3. *Il est associatif.*
4. *Il est distributif par rapport à la somme.*
5. *Son élément neutre est la suite $X^0 = (\delta_{0\,j})_{j\in\mathbb{N}}$.*
   (Que vaut $\deg(X^0)$?)
6. *La suite nulle est l'élément absorbant ; c'est à dire : le produit de toute suite par la suite nulle donne la suite nulle.*

L'ensemble $\mathbb{K}[X]$ muni du produit défini ci-dessus est un monoïde commutatif. Ce même ensemble muni des deux lois somme et produit définies ci-dessus est un anneau commutatif.

Théorème 3.1.2

$$(\forall u \in \mathbb{K}[X])\,(\forall v \in \mathbb{K}[X]) \quad \deg(uv) = \deg(u) + \deg(v)$$

Démonstration 3.1.2 Si u ou v est la suite nulle, alors uv est aussi la suite nulle et l'égalité $\deg(uv) = \deg(u)+\deg(v)$ est vraie.
Supposons que ni u, ni v, ne soit la suite nulle. Dans ce cas, $\deg(u)$ et $\deg(v)$ sont des nombres entiers. Notons ces nombres respectivement m et n, et montrons que $(uv)_{m+n} \neq 0$.
Par définition de produit, $(uv)_{m+n} = \sum_{p+q=m+n} u_p v_q$. Or, si $p+q = m+n$ et $p < m$, alors $q > n$ et donc $v_q = 0$. De même, $p+q = m+n$ et $p > m$ impliquent $q < m$ et $u_p = 0$. Si $p+q = m+n$ et $p = m$, alors $q = n$ et $u_p v_q = u_m v_n \neq 0$. D'où :

$$\begin{aligned}(uv)_{m+n} &= \sum_{p+q=m+n} u_p v_q = \sum_{\substack{p+q=m+n \\ p<m \quad q>n}} u_p v_q + \sum_{\substack{p+q=m+n \\ p>m \quad q<n}} u_p v_q + \sum_{\substack{p+q=m+n \\ p=m \quad q=n}} u_p v_q \\ &= \sum_{\substack{p+q=m+n \\ p<m \quad q>n}} u_p 0 + \sum_{\substack{p+q=m+n \\ p>m \quad q<n}} 0 v_q + u_m v_n = u_m v_n \neq 0\end{aligned}$$

Donc, nous avons obtenu : $\deg(uv) \geqslant \deg(u) + deg(v)$.
Montrons que : $(uv)_k = 0$ pour tout entier $k > m+n$.
Soit $k > m+n$. Si $p+q = k$ et $p \leqslant m$, alors $q = k-p \geqslant k-m > m+n-m = n$ et donc $v_q = 0$. On en déduit :

$$\begin{aligned}(uv)_k &= \sum_{p+q=k} u_p v_q = \sum_{\substack{p+q=k \\ p\leqslant m}} u_p v_q + \sum_{\substack{p+q=k \\ p>m}} u_p v_q \\ &= \sum_{\substack{p+q=k \\ p\leqslant m}} u_p 0 + \sum_{\substack{p+q=k \\ p>m}} 0 v_q = 0\end{aligned}$$

Cette fois nous venons d'obtenir : $\deg(uv) \leqslant \deg(u) + \deg(v)$.
De $\deg(uv) \geqslant \deg(u) + deg(v)$ et $\deg(uv) \leqslant \deg(u) + deg(v)$, on déduit l'égalité.

4. La notation $\sum_{i+j=n} u_i v_j$ désigne la somme de tous les $u_i v_j$ tels que les nombres entiers naturels i et j vérifient $i+j = n$. On rencontre aussi $\sum_{i\in\mathcal{I}} a_i$ qu'il faut interpréter comme : la somme de tous les a_i, i décrivant l'ensemble $\mathcal{I}$.

Corollaire 3.1.2.1 *Notons $\mathbb{K}[X]^*$ l'ensemble des éléments inversibles de $\mathbb{K}[X]$ pour le produit (pour la loi produit). On a :*

$$\mathbb{K}[X]^* = \{u \in \mathbb{K}[X] \mid \deg(u) = 0\}$$

Démonstration 3.1.2.1 Première partie : $\mathbb{K}[X]^* \subset \{u \in \mathbb{K}[X] \mid \deg(u) = 0\}$.
Soit $u \in \mathbb{K}[X]^*$. Montrons que $\deg(u) = 0$.
Si $u \in \mathbb{K}[X]^*$, alors il existe $v \in \mathbb{K}[X]^*$ tel que : $uv = X^0$. D'après le théorème : $\deg(uv) = \deg(u) + \deg(v)$. D'autre part, $\deg(X^0) = 0$. De $\deg(u) + \deg(v) = 0$, on déduit : $\deg(u) = \deg(v) = 0$.
Deuxième partie : $\mathbb{K}[X]^* \supset \{u \in \mathbb{K}[X] \mid \deg(u) = 0\}$.
Soit $u \in \mathbb{K}[X]$ tel que $\deg(u) = 0$. Montrons que $u \in \mathbb{K}[X]^*$.
Si $\deg(u) = 0$, alors $u_n = 0$ pour $n \geqslant 1$ et $u_0 \neq 0$. Or, si $u_0 \neq 0$, alors u_0 est un élément de $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$, dont l'inverse est noté : u_0^{-1}. Soit $v \in \mathbb{K}[X]$ définie par : $v_n = 0$ si $n \geqslant 1$, et $v_0 = u_0^{-1}$. Alors, $(uv)_0 = \sum_{p+q=0} u_p v_q = u_0 v_0 = 1$ et, pour $n \geqslant 1$, $(uv)_n = \sum_{p+q=n} u_p v_q = u_0 v_n + \sum_{\substack{p+q=n \\ p \neq 0}} u_p v_q = u_0 0 + \sum_{\substack{p+q=n \\ p \neq 0}} 0 v_q = 0$. Donc, $uv = X^0$ et u est inversible.

Multiplication par les éléments de $\mathbb{K}$

Définition et notation 3.1.14 (Produit d'une suite par un nombre) *Soient $u \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On note le produit de u par λ : λu. Ce produit est la suite presque nulle définie par : $(\lambda u)_n = \lambda u_n$.*

Exercice 3.1.4 *Pour tout $u \in \mathbb{K}[X]$, tout $v \in \mathbb{K}[X]$, tout $\lambda \in \mathbb{K}$ et tout $\mu \in \mathbb{K}$, montrer que :*

1. $\lambda(u + v) = \lambda u + \lambda v$
2. $\lambda(uv) = (\lambda u)v = u(\lambda v)$
3. $(\lambda\mu)u = \lambda(\mu u) = \mu(\lambda u)$
4. $(\lambda + \mu)u = \lambda u + \mu u$
5. $1u = u$
6. $0u = (0)_{n\in\mathbb{N}}$
7. $\lambda\,(0)_{n\in\mathbb{N}} = (0)_{n\in\mathbb{N}}$

$\mathbb{K}[X]$ muni de la somme et de la multiplication par les éléments de $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel.
$\mathbb{K}[X]$ muni de la somme, du produit et de la multiplication par les éléments de $\mathbb{K}$ est une $\mathbb{K}$-algèbre commutative.

3.1.3 Polynômes à coefficients dans $\mathbb{K}$

Une suite remarquable d'éléments de $\mathbb{K}[X]$

Définition et notation 3.1.15 *La suite $X^n \in \mathbb{K}[X]$ est définie pour tout $n \in \mathbb{N}$ par :*

$$X^n = (\delta_{n\,j})_{j\in\mathbb{N}}$$

Exercice 3.1.5 *Pour tout $m \in \mathbb{N}$ et tout $n \in \mathbb{N}$, montrer que :*

1. $\deg(X^n) = n$
2. $X^m X^n = X^{m+n}$
3. $(X^m)^n = \underbrace{X^m X^m \cdots X^m}_{\substack{\text{produit de } n \\ \text{copies de } X^m}} = X^{mn}$

L'exercice 3.1.5 justifie la notation X^n. On remarque en effet que les règles de calcul dans $\mathbb{K}$ sur les exposants sont transposables aux X^n.

Définition 3.1.16 (Combinaison linéaire) *Soit $U = ({}^n u)_{n\in\mathbb{N}}$ une suite [5] d'éléments de $\mathbb{K}[X]$. Soit $\lambda = (\lambda_n)_{n\in\mathbb{N}}$ une suite presque nulle d'éléments de $\mathbb{K}$. Alors, la somme : $\sum_{n\in\mathbb{N}} \lambda_n\, {}^n u$, est ce qu'on appelle une combinaison linéaire de la famille $({}^n u)_{n\in\mathbb{N}}$. (On dit aussi : combinaison linéaire des ${}^n u$).*

Remarque : la somme de la définition ci-dessus comporte un nombre fini de termes car, la suite λ étant presque nulle, donc tous les termes, sauf un nombre fini d'entre eux, sont nuls.

Exercice 3.1.6 *Montrer que toute combinaison linéaire d'une famille de suites presque nulles est une suite presque nulle.*

5. L'indice n est volontairement placé devant u pour distinguer ${}^n u$ élément de $\mathbb{K}[X]$, de u_n qui désignait jusque là un élément de $\mathbb{K}$. U est une suite de suites.

Théorème 3.1.3 *Tout élément de $\mathbb{K}[X]$ s'exprime de manière unique (la suite λ de la définition 3.1.16 est uniquement déterminée) comme combinaison linéaire de la famille $(X^n)_{n\in\mathbb{N}}$.*

Démonstration 3.1.3 Existence :
Si $u = (u_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$, alors $u = \sum_{n\in\mathbb{N}} u_n X^n$. En effet, le terme de rang m de la suite $\sum_{n\in\mathbb{N}} u_n X^n$ est la somme des termes de rang m des suites u_0X^0, u_1X^1, u_2X^2, etc. D'où : $\left(\sum_{n\in\mathbb{N}} u_n X^n\right)_m = \sum_{n\in\mathbb{N}} u_n X^n_m = \sum_{n\in\mathbb{N}} u_n \delta_{n\,m} = u_m$, car tous les $\delta_{n\,m}$ sont nuls, sauf $\delta_{m\,m}$qui vaut 1. La suite λ utilisée dans la définition 3.1.16 est donc ici la suite u elle-même.
Unicité :
Soit $\lambda \in \mathbb{K}[X]$. Supposons $u = \sum_{n\in\mathbb{N}} \lambda_n X^n$. Alors, le terme de rang m de $\sum_{n\in\mathbb{N}} \lambda_n X^n$ est λ_m. Comme on a supposé $u = \sum_{n\in\mathbb{N}} \lambda_n X^n$, le terme de rang m est u_m. Donc, pour tout $m \in \mathbb{N}$, on obtient $\lambda_m = u_m$, d'où l'unicité.

La définition de combinaison linéaire que nous nous sommes donnés, convient à la situation dans laquelle sont les X^n.

L'anneau $\mathbb{K}[X]$ des polynômes

Proposition 3.1.4 *L'application :*

$$\begin{aligned} \phi : \mathbb{K} &\to \mathbb{K}[X] \\ \lambda &\mapsto \lambda X^0 \end{aligned}$$

est injective.

Démonstration 3.1.4 $\lambda X^0 = \mu X^0 \Rightarrow (\lambda X^0)_0 = (\mu X^0)_0 \Rightarrow \lambda = \mu$

Pour $\lambda \in \mathbb{K}$, par abus de notation, l'élément λX^0 de $\mathbb{K}[X]$ est noté simplement λ. Cet abus est dû à la proposition ci-dessus. Puisque qu'il existe une injection "canonique" de $\mathbb{K}$ dans $\mathbb{K}[X]$, on considère $\mathbb{K}$ comme un sous-ensemble de $\mathbb{K}[X]$, bien qu'il n'en soit pas un en réalité ; c'est $\phi(\mathbb{K})$ qui est inclus dans $\mathbb{K}[X]$.
La notation simplifiée de X^0 est 1, celle de X^1 est X.
La suite nulle sera tout simplement notée 0.
Cet abus, ces simplifications, et le théorème 3.1.3, nous permettent de retrouver l'écriture usuelle des éléments de $\mathbb{K}[X]$, qui sont les polynômes à une indéterminée.
Par exemple : $P(X) = 1 + 2X - X^3$ est un polynôme. C'est la suite presque nulle d'éléments de $\mathbb{K}$ dont les termes sont :
$P(X)_0 = 1$, $P(X)_1 = 2$, $P(X)_2 = 0$, $P(X)_3 = -1$, et pour tout entier n supérieur ou égal à 4 : $P(X)_n = 0$.

Définition 3.1.17 *$\mathbb{K}[X]$ est l'anneau des polynômes à une indéterminée et à coefficients dans $\mathbb{K}$.*

Partout où sont écrit les mots "suite presque nulle", vous pouvez écrire à la place "polynôme". Les divers définitions, propositions et théorèmes sur les suites presque nulles, sont donc en fait des définitions, propositions et théorèmes sur les polynômes. Ce détour par les suites presque nulles est, par exemple, une des meilleures façons de définir sans ambiguïté le degré d'un polynôme, ou bien la forme canonique d'un polynôme.

Définition 3.1.18 (Forme canonique) *Soit $P \in \mathbb{K}[X]$. On sait (théorème 3.1.3) que P s'écrit de façon unique comme une combinaison linéaire des X^n. Cette combinaison linéaire est la forme canonique de P.*

Notation 3.1.19 *Soit $P \in \mathbb{K}[X]$. Considérons sa forme canonique :*

$$P = \sum_{n\in\mathbb{N}} a_n X^n.$$

Si $P = 0$, alors on écrira la forme canonique de P : 0 ou $\sum_{n=0}^{0} 0$ lorsque la notation [6] $\sum$ sera utilisée.
Si $P \neq 0$, alors $\deg(P) \in \mathbb{N}$ et dans ce cas on écrira la forme canonique de P : $\sum_{n=0}^{\deg(P)} a_n X^n$.

Définition 3.1.20 (Coefficients) *Les termes de la suite $(a_n)_{n\in\mathbb{N}}$ utilisée dans la notation 3.1.19 s'appellent les coefficients de P.*

Définition 3.1.21 (Monôme) *Un polynôme dont la forme canonique est réduite, pour un certain $n \in \mathbb{N}$, à aX^n, avec $a \in \mathbb{K}$, est un monôme.*

6. Un autre point de vue consiste à penser que $\sum_{n=0}^{-\infty} = \sum_{n\in\emptyset} = 0$.

Remarque : noter un polynôme $P(X)$ ou P est indifférent, sauf, par exemple, lorsqu'on écrit : $P = XY$. Est-ce que l'indéterminée du polynôme est X ? Est-ce Y ? Est-ce un polynôme à deux [7] indéterminées ?
Écrire $P(X)$ et $Q(X)$ permet de composer ces polynômes pour en fabriquer de nouveaux, comme : $P(Q(X))$. Si $P(X) = -1 + X^2$ et $Q(X) = 1 + X$, alors $P(Q(X)) = -1 + (Q(X))^2 = -1 + (1 + X)^2 = -1 + 1 + 2X + X^2 = 2X + X^2$. Les exposants qui figurent dans ces expressions peuvent être différemment interprétés. $(Q(X))^2$ doit être interprété comme : $Q(X)Q(X)$. X^2 peut être interprété comme : $(\delta_{2\,j})_{j\in\mathbb{N}}$, mais aussi (exercice 3.1.5) comme : XX.

3.2 Division euclidienne dans $\mathbb{K}[X]$

Les outils utilisés dans cette section sont ceux de la théorie des anneaux commutatifs intègres ; outils de l'algèbre « abstraite » qui permettent, sans trop d'efforts, d'obtenir les principaux résultats du programme. Les techniques développées pourront être transposées à une étude plus générale des anneaux commutatifs intègres, étude au programme des second cycle de mathématiques.

3.2.1 Division euclidienne

Théorème 3.2.1 *Pour tout P et tout Q dans $\mathbb{K}[X]$:*

$$PQ = 0 \iff (P = 0 \text{ ou } Q = 0)$$

Démonstration 3.2.1 Posons $Q = (q_n)_{n\in\mathbb{N}}$ et $PQ = (a_n)_{n\in\mathbb{N}}$. Si $P = 0$, alors $a_n = \sum_{i+j=n} 0q_j = 0$. Donc, $P = 0 \Rightarrow PQ = 0$. De même, on montre que $Q = 0 \Rightarrow PQ = 0$.
Réciproquement :
Si $PQ = 0$, alors le théorème 3.1.2 sur le degré du produit permet d'affirmer : $-\infty = \deg(PQ) = \deg(P) + \deg(Q)$. Or, si $P \neq 0$ et $Q \neq 0$, alors $\deg(P)$ et $\deg(Q)$ sont des nombres entiers dont la somme ne peut valoir $-\infty$. D'où le résultat.

Bien que l'étude des structures algébriques abstraites ne soit pas un objectif de ce cours, signalons qu'un anneau vérifiant le théorème 3.2.1 s'appelle un anneau intègre. Par exemple, $\mathbb{Z}$ est un anneau intègre : un produit de nombres entiers est nul si et seulement si un des facteurs du produit est nul. Le théorème 3.2.1 étant établi, nous pouvons envisager la division euclidienne dans $\mathbb{K}[X]$, fondée grâce au théorème 3.2.2.

Théorème 3.2.2 Division euclidienne dans $\mathbb{K}[X]$
Soient A et B des éléments de $\mathbb{K}[X]$. On suppose $B \neq 0$.
Il existe alors dans $\mathbb{K}[X]^2$ un unique couple de polynômes (Q, R) tel que : $A = BQ + R$ et $\deg(R) < \deg(B)$.
Q est le quotient, et R le reste, de la division euclidienne de A par B.

Démonstration 3.2.2 Montrons par récurrence sur le degré de A, l'existence d'un couple (Q, R) vérifiant $A = BQ+R$ et $\deg(R) < m$.
Notons m le degré de B ($B \neq 0 \Rightarrow m \in \mathbb{N}$). Si $\deg(A) < m$, alors le couple $(Q, R) = (0, A)$ convient. (Ceci règle en particulier le cas $A = 0$).
Hypothèse de récurrence : pour tout polynôme A de degré inférieur ou égal à n, il existe un couple de polynômes (Q, R) tel que $A = BQ + R$ et $\deg(R) < m$.
Soit A un polynôme de degré $n+1$. Si $n+1 < m$ le choix est $Q = 0$ et $R = A$. Sinon, on a : $m \leqslant n+1$. Considérons les formes canoniques de A et de B : $A = \sum_{i=0}^{n+1} a_i X^i$ et $B = \sum_{i=0}^{m} b_i X^i$. Posons $C = A - \left(\frac{a_{n+1}}{b_m} X^{n+1-m}\right) B$. C est un polynôme bien défini, puisque $b_m \neq 0$ et $m \leqslant n+1$. D'après les théorèmes 3.1.1 et 3.1.2, $\deg(C) \leqslant n+1$. Or, d'après la définition de C, le monôme de degré $n+1$ de la forme canonique de C est nul. D'où, $\deg(C) \leqslant n$. On peut donc appliquer l'hypothèse de récurrence à C. On en déduit l'existence d'un couple de polynômes (Q_1, R_1) tels que $C = BQ_1 + R_1$ et $\deg(R_1) < m$. Comme $C = A - \left(\frac{a_{n+1}}{b_m} X^{n+1-m}\right) B$, on obtient : $A = \left(\frac{a_{n+1}}{b_m} X^{n+1-m} + Q_1\right) B + R_1$. Les polynômes $Q = \frac{a_{n+1}}{b_m} X^{n+1-m} + Q_1$ et $R = R_1$ vérifient $A = BQ + R$ et $\deg(R) < m$.
Conclusion : l'existence du couple (Q, R) est démontrée.

7. Ces polynômes ne seront pas étudiés dans ce cours.

Montrons l'unicité du couple (Q, R).
Supposons $A = BQ + R = BQ_1 + R_1$ avec $\deg(R) < m$ et $\deg(R_1) < m$. Alors, $(Q - Q_1)B = R_1 - R$ et d'après les théorèmes 3.1.2 et 3.1.1 :

$$\begin{aligned} m &> \max\{\deg(R_1), \deg(R)\} \geqslant \deg(R_1 - R) \\ &= \deg((Q - Q_1)B) = \deg(Q_1 - Q) + m \end{aligned}$$

D'où, $\deg(Q_1 - Q) = -\infty$, et donc $Q = Q_1$. Comme $R_1 - R = (Q - Q_1)B$, on en déduit : $R = R_1$.

3.2.2 $\mathbb{K}[X]$ est principal

Définition 3.2.1 (Idéal) *Soit $\mathcal{I} \subset \mathbb{K}[X]$. On dit que $\mathcal{I}$ est un idéal de $\mathbb{K}[X]$, si $\mathcal{I}$ vérifie toutes les propriétés suivantes :*

1. $\mathcal{I} \neq \emptyset$
2. $(\forall P \in \mathbb{K}[X]) \quad P \in \mathcal{I} \Rightarrow -P \in \mathcal{I}$
3. $(\forall P \in \mathbb{K}[X])(\forall Q \in \mathbb{K}[X]) \quad (P \in \mathcal{I} \text{ et } Q \in \mathcal{I}) \Rightarrow P + Q \in \mathcal{I}$
4. $(\forall P \in \mathbb{K}[X])(\forall Q \in \mathbb{K}[X]) \quad P \in \mathcal{I} \Rightarrow PQ \in \mathcal{I}$

Remarque : $\{0\}$ et $\mathbb{K}[X]$ sont deux idéaux de $\mathbb{K}[X]$.

Proposition 3.2.3 *Soit $\mathfrak{S}$ un ensemble non vide. Soit $(\mathcal{I}_s)_{s\in\mathfrak{S}}$ une famille d'idéaux de $\mathbb{K}[X]$. Alors, $\mathcal{I} = \bigcap_{s\in\mathfrak{S}} \mathcal{I}_s$ est un idéal de $\mathbb{K}[X]$.*

Démonstration 3.2.3 Il faut examiner si $\mathcal{I}$ vérifie bien la définition 3.2.1. La première vérification consiste à observer que $\mathcal{I}$ n'est pas vide. Comme 0 appartient à tous les idéaux de $\mathbb{K}[X]$ (preuve?), 0 est dans n'importe quelle intersection d'idéaux, donc dans $\mathcal{I}$. Montrons que le second axiome de la définition est vérifié par $\mathcal{I}$. Les autres axiomes sont à vérifier en suivant la même démarche (exercice).
Soit $P \in \mathcal{I}$. Alors, comme $\bigcap_{s\in\mathfrak{S}} \mathcal{I}_s$ est l'intersection de tous les $\mathcal{I}_s$ pour $s \in \mathfrak{S}$, P appartient à tous les $\mathcal{I}_s$. Comme les $\mathcal{I}_s$ sont tous des idéaux, de $P \in \mathcal{I}_s$, on déduit $-P \in \mathcal{I}_s$. Puisque pour tout $s \in \mathfrak{S}$, $-P \in \mathcal{I}_s$, on a : $-P \in \bigcap_{s\in\mathfrak{S}} \mathcal{I}_s = \mathcal{I}$.

Proposition 3.2.4 *Soit $\mathcal{I}$ un idéal de $\mathbb{K}[X]$.*
$\mathcal{I} = \mathbb{K}[X]$ si et seulement si, il existe un élément inversible (pour le produit) dans $\mathcal{I}$.

Démonstration 3.2.4 Supposons $\mathcal{I} = \mathbb{K}[X]$. Alors, tous les éléments inversibles de $\mathbb{K}[X]$ appartiennent à $\mathcal{I}$.
Réciproquement, s'il existe dans $\mathcal{I}$ un élément inversible λ, alors d'après la définition 3.2.1, pour tout polynôme P de $\mathbb{K}[X]$, $\lambda\lambda^{-1}P = P \in \mathcal{I}$. D'où, $\mathcal{I} = \mathbb{K}[X]$.

Notation 3.2.2 *Soit P un élément de $\mathbb{K}[X]$. On note (P) le sous-ensemble de $\mathbb{K}[X]$ défini par :*

$$(P) = \{A \in \mathbb{K}[X] \mid (\exists Q \in \mathbb{K}[X]) \quad A = PQ\}$$

Exercice 3.2.1 *Montrer que : $(P) = \{0\} \iff P = 0$.*

Proposition 3.2.5 *(P) (voir notation 3.2.2) est un idéal de $\mathbb{K}[X]$. On l'appelle : l'idéal engendré par P.*

Démonstration 3.2.5 $(P) \neq \emptyset$, car $P \times 0 = 0 \in (P)$.
Soit $A \in (P)$. Il existe $Q \in \mathbb{K}[X]$ tel que $A = PQ$. Comme $-A = P(-Q)$, on a : $-A \in (P)$.
Soient A et B dans (P). Il existe des polynômes Q_1 et Q_2 tels : $A = PQ_1$ et $B = PQ_2$. Alors, $A+B = P(Q_1+Q_2) \in (P)$.
Soit $A = PQ \in (P)$ et $B \in \mathbb{K}[X]$. Alors, $AB = (PQ)B = P(QB) \in (P)$.

Exercice 3.2.2 *Soit $\mathcal{I}$ un idéal de $\mathbb{K}[X]$. Montrer que $P \in \mathcal{I}$ équivaut à $(P) \subset \mathcal{I}$.*

Proposition 3.2.6 *(P) est l'intersection de tous les idéaux ayant P pour élément. Autrement dit : (P) est le plus petit des idéaux de $\mathbb{K}[X]$ ayant P pour élément.*

Démonstration 3.2.6 Comme (P) est un idéal ayant P pour élément, l'intersection de tous les idéaux ayant P pour élément est incluse dans (P). Réciproquement, d'après l'exercice 3.2.2, (P) est inclus dans tout idéal ayant P pour élément. Donc, (P) est inclus dans l'intersection de tous les idéaux ayant P pour élément.

Proposition 3.2.7 *$(P) = (Q)$ si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$.*

Démonstration 3.2.7 S'il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$, alors $P = Q(\lambda X^0) \in (Q)$. D'où, d'après l'exercice 3.2.2, $(P) \subset (Q)$. Comme $\lambda \neq 0$, de $P = \lambda Q$, on déduit $Q = \lambda^{-1}P$, et donc $(Q) \subset (P)$. Comme $(P) \subset (Q)$ et $(Q) \subset (P)$, on a : $(P) = (Q)$.
Réciproquement : supposons $(P) = (Q)$. Alors, $P \in (Q)$. De même, $Q \in (P)$. Il existe donc des polynômes A et B, tels que $P = QA$ et $Q = PB$. Mais alors : $P = QA = (PB)A$, et, d'après le théorème 3.1.2, $\deg(P) = \deg(P) + \deg(A) + \deg(B)$. Cette égalité implique $\deg(P) = -\infty$, ou $\deg(A) = \deg(B) = 0$. Si $P = 0$, alors $(P) = \{0\}$ et donc Q qui appartient à (P), ne peut être que 0. Dans ce cas, pour tout λ dans $\mathbb{K}$, $P = \lambda Q$. Si $P \neq 0$, alors $\deg(A) = \deg(B) = 0$ et donc, d'après le corollaire 3.1.2.1, A et B sont inversibles (pour le produit dans $\mathbb{K}[X]$). On a donc $A = \lambda X^0$ avec $\lambda \in \mathbb{K}^*$. Mais alors $P = QA = AQ = \lambda X^0 Q = \lambda Q$.

Définition 3.2.3 (Idéal principal) *Soit $\mathcal{I}$ un idéal de $\mathbb{K}[X]$.*
On dit que $\mathcal{I}$ est un idéal principal s'il existe P dans $\mathbb{K}[X]$ tel que : $\mathcal{I} = (P)$.

Théorème 3.2.8 *Tout idéal de $\mathbb{K}[X]$ est principal.*

Démonstration 3.2.8 Soit $\mathcal{I}$ un idéal de $\mathbb{K}[X]$.
Si $\mathcal{I} = \{0\}$, alors $\mathcal{I} = (0)$.
Supposons $\mathcal{I} \neq \{0\}$. Alors, $\mathcal{I} \setminus \{0\} \neq \emptyset$. Soit Δ un polynôme de $\mathcal{I} \setminus \{0\}$ vérifiant [8] : $\deg(\Delta) = \min\{\deg(P) \in \mathbb{N} \mid P \in \mathcal{I} \setminus \{0\}\}$. D'après l'exercice 3.2.2, $(\Delta) \subset \mathcal{I}$. Soit $A \in \mathcal{I}$. D'après le théorème 3.2.2, il existe un unique couple de polynômes (Q, R) tel que : $A = \Delta Q + R$ et $\deg(R) < \deg(\Delta)$. Comme Δ et A sont des éléments de $\mathcal{I}$, et que $\mathcal{I}$ est un idéal, on a : $R = A - \Delta Q \in \mathcal{I}$. De $R \in \mathcal{I}$, $\deg(\Delta) = \min\{\deg(P) \in \mathbb{N} \mid P \in \mathcal{I} \setminus \{0\}\}$ et $\deg(R) < \deg(\Delta)$, on déduit : $R = 0$. D'où $A = \Delta Q$, et donc $\mathcal{I} \subset (\Delta)$. Comme, d'autre part, $(\Delta) \subset \mathcal{I}$, on obtient : $\mathcal{I} = (\Delta)$.

Un anneau intègre dont tout idéal est principal s'appelle un anneau principal. Nous avons donc démontré que $\mathbb{K}[X]$ est principal.

PGCD

Exercice 3.2.3 *Posons :*

$$(A,B) = \{P \in \mathbb{K}[X] \mid (\exists U \in \mathbb{K}[X])(\exists V \in \mathbb{K}[X]) \quad P = AU + BV\}.$$

Montrer que (A,B) est le plus petit des idéaux de $\mathbb{K}[X]$ ayant A et B pour éléments. (A,B) est l'idéal engendré par A et B.

Définition et notation 3.2.4 (Diviseur) *Soient A et B dans $\mathbb{K}[X]$. On dit que B divise A (B est un diviseur [9] de A), s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$. "B divise A" se note : $B|A$.*

Exercice 3.2.4 *Montrer que A est inversible ($A \in \mathbb{K}[X]^*$) si et seulement si tout diviseur de A est inversible.*

Exercice 3.2.5 *Montrer que :*

1. *$B|A$ et $B = 0$ impliquent $A = 0$.*
2. *Pour tout $\lambda \in \mathbb{K}^*$ et tout $P \in \mathbb{K}[X]$: $\lambda|P$. ($\lambda = \lambda X^0$)*
3. *Pour $B \neq 0$, $B|A$ si et seulement si le reste de la division euclidienne de A par B est nul.*
4. *$B|A \iff (A) \subset (B) \iff A \in (B)$.*
5. *Si $A|B$ et $A|C$, alors $A|B + C$.*
6. *Si $A|B$ alors $AC|BC$.*

Définition 3.2.5 (PGCD) *Soient A et B des éléments de $\mathbb{K}[X]$. On dit que $\Delta \in \mathbb{K}[X]$ est un PGCD [10] de A et de B, si Δ vérifie :*

1. *$\Delta|A$*
2. *$\Delta|B$*
3. *$(\forall P \in \mathbb{K}[X]) \quad (P|A \text{ et } P|B) \Rightarrow P|\Delta$*

8. Pour un sous-ensemble non vide $\mathcal{E}$ de $\mathbb{R}$, $\min \mathcal{E}$ désigne, s'il existe, le minimum de $\mathcal{E}$, c'est à dire : son plus petit élément.
9. Un cas particulier d'emploi du terme « diviseur » : « diviseur de 0 », désigne dans les anneaux qui ne sont pas intègres les éléments $a \neq 0$ tels qu'il existe $b \neq 0$ vérifiant $ab = 0$. Pour nous, dans le cadre des anneaux intègres, il n'existe aucun élément différent de 0 dont le produit avec un élément différent de 0 a pour valeur 0.
10. "Plus Grand Commun Diviseur"

Un PGCD de A et de B est donc un polynôme qui divise A et B, et tout diviseur de A et de B divise le PGCD.

Théorème 3.2.9 *Soient A, B et Δ des éléments de $\mathbb{K}[X]$.*
Δ est un PGCD de A et de B si et seulement si $(A,B) = (\Delta)$.

La définition 3.2.5 donne du PGCD une définition qui traduit directement "plus grand commun diviseur" ; avec "plus grand" qui doit être compris comme : tout diviseur commun divise un PGCD. Le théorème 3.2.9 pourrait être une définition du PGCD en termes d'idéaux, puisqu'il indique qu'un PGCD de A et de B est un polynôme qui engendre le même idéal que celui engendré par A et B. L'avantage du théorème sur la définition, c'est qu'il implique l'existence d'un PGCD, alors que la définition ne garantie pas qu'il en existe un. En effet, comme $\mathbb{K}[X]$ est principal, il existe, quels que soient les polynômes A et B, un polynôme Δ tel que $(A,B) = (\Delta)$.

Démonstration 3.2.9 Soit Δ un PGCD de A et de B.
Puisque $\Delta|A$, il existe $S \in \mathbb{K}[X]$ tel que $A = \Delta S$. De même comme $\Delta|B$, il existe $T \in \mathbb{K}[X]$ tel que $B = \Delta T$. Comme $\mathbb{K}[X]$ est principal, il existe $C \in \mathbb{K}[X]$ tel que $(C) = (A,B)$. De $C \in (C) = (A,B)$, on déduit l'existence de polynômes U et V tels que $C = AU + BV$. Mais alors, $C = AU + BV = \Delta TU + \Delta SV = \Delta(TU + SV)$, et donc : $C \in (\Delta)$. D'où $(A,B) = (C) \subset (\Delta)$.
Comme $A \in (A,B) = (C)$, on a : $C|A$. De même, $C|B$. Mais alors, comme Δ est un PGCD de A et de B, $C|\Delta$. D'où, $\Delta \in (C)$ et donc $(\Delta) \subset (C) = (A,B)$.
De $(A,B) = (C) \subset (\Delta)$ et $(\Delta) \subset (C) = (A,B)$, on déduit : $(A,B) = (\Delta)$.

Réciproquement, supposons $(A,B) = (\Delta)$. Alors $A \in (\Delta)$ et $B \in (\Delta)$; autrement dit : $\Delta|A$ et $\Delta|B$. Soit P un diviseur commun à A et à B. Il existe des polynômes F et G tels que $A = PF$ et $B = PG$. Comme $\Delta \in (A,B)$, il existe des polynômes W et Z tels que $\Delta = AW + BZ$. Alors, $\Delta = AW + BZ = PFW + PGZ = P(FW + GZ)$; c'est à dire : $P|\Delta$. Donc, Δ est un PGCD de A et de B.

Corollaire 3.2.9.1 *Soient A, B, Δ et D dans $\mathbb{K}[X]$.*
Δ et D sont des PGCD de A et de B si, et seulement si, Δ est un PGCD de A et de B et il existe $\lambda \in \mathbb{K}^*$ tel que $\Delta = \lambda D$.

Démonstration 3.2.9.1 Supposons que Δ et D soient des PGCD de A et de B. D'après le théorème 3.2.9, ceci équivaut à : $(A,B) = (\Delta) = (D)$. D'après la proposition 3.2.7, $(\Delta) = (D)$ équivaut à : il existe λ dans $\mathbb{K}^*$ tel que $\Delta = \lambda D$. D'où le corollaire.

Ce corollaire indique pourquoi nous n'avons pas défini le PGCD, mais un PGCD. En effet, le PGCD n'est défini qu'à la multiplication par les éléments de $\mathbb{K}^*$ près.

Définition 3.2.6 (Polynômes premiers entre eux) *Soient A et B dans $\mathbb{K}[X]$. On dit que A et B sont premiers entre eux si leurs seuls diviseurs communs sont les éléments de $\mathbb{K}^*$ (en identifiant $\lambda \in \mathbb{K}^*$ à $\lambda X^0 \in \mathbb{K}[X]^*$).*

Exercice 3.2.6 *Montret que $A = 0$ et A et B sont premier entre eux, alors $B \in \mathbb{K}^*$*

Théorème 3.2.10 (Bezout) *Soient A et B des éléments de $\mathbb{K}[X]$.*
A et B sont premiers entre eux si et seulement si, il existe des polynômes U et V de $\mathbb{K}[X]$, tels que : $AU+BV = 1$.

Démonstration 3.2.10 Rappelons que $AU + BV = 1$ devrait s'écrire $AU + BV = X^0$. D'après le théorème 3.2.9, un PGCD de A et de B est un polynôme Δ tel que $(\Delta) = (A,B)$. Si A et B sont premiers entre eux, alors leurs PGCD, qui appartiennent tous à (A,B), sont les éléments de $\mathbb{K}^*$, car ce sont leurs seuls diviseurs communs, et alors $(A,B) = \mathbb{K}[X]$. De $1 \in (A,B)$, on déduit l'existence de polynômes U et V tels que $AU + BV = 1$.
Réciproquement, s'il existe des polynômes U et V tels que $AU + BV = 1$, alors $1 \in (A,B)$ et donc $(A,B) = (1) = \mathbb{K}[X]$. Si P est un diviseur commun à A et à B, alors $A \in (P)$ et $B \in (P)$. D'où $(A,B) \subset (P)$ (voir execice 3.2.3). Comme $(A,B) = \mathbb{K}[X]$, on a $(P) = \mathbb{K}[X]$, et donc P est un élément inversible de $\mathbb{K}[X]$, car $1 \in (P)$ implique l'existence d'un polynôme Q tel que $1 = PQ$.

Théorème 3.2.11 (Gauss) *On considère les polynômes A, B et C de $\mathbb{K}[X]$.*
Si A et B sont premiers entre eux et si $A|BC$, alors $A|C$.

Démonstration 3.2.11 D'après le théorème de Bezout, il existe des polynômes U et V dans $\mathbb{K}[X]$ tels que $AU+BV = 1$. D'où $AUC+BVC = C$. Comme $A|BC$, il existe Q tel que $BC = AQ$. Alors, $C = AUC+BCV = AUC+AQC = A(UC + QC)$, et donc $A|C$.

PPCM

Définition 3.2.7 (multiple) *Soient A et B dans $\mathbb{K}[X]$. On dit que A est un multiple de B, si $B|A$.*

Exercice 3.2.7 *Montrer que 0 est un multiple de P, quel que soit P dans $\mathbb{K}[X]$.*

Définition 3.2.8 (PPCM) *Soient A, B et M dans $\mathbb{K}[X]$.*
On dit que M est un PPCM[11] *de A et de B si M vérifie :*

1. *M est un multiple de A.*
2. *M est un multiple de B.*
3. *Pour tout P dans $\mathbb{K}[X]$, si P est un multiple commun à A et à B, alors P est un multiple de M.*

Théorème 3.2.12 *Soient A, B et M dans $\mathbb{K}[X]$.*
M est un PPCM de A et de B si et seulement si $(M) = (A) \cap (B)$.

Le théorème 3.2.12 donne une définition du PPCM en termes d'idéaux, et garantit l'existence d'un PPCM, car l'intersection de deux idéaux est un idéal et $\mathbb{K}[X]$ est principal. Ce théorème et la proposition 3.2.7 page 28, justifient l'emploi du terme « un PPCM », car le PPCM n'est défini qu'à la multiplication par un élément de $\mathbb{K}^*$ près.

Démonstration 3.2.12 Soit P un multiple commun à A et à B. De $A|P$ et $B|P$, on déduit $P \in (A)$ et $P \in (B)$, donc $(P) \subset (A) \cap (B)$. D'où, si M est un PPCM de A et de B : $(M) \subset (A) \cap (B)$. $\mathbb{K}[X]$ étant principal, il existe un polynôme C tel que $(C) = (A) \cap (B)$. Comme $C \in (A)$ et $C \in (B)$, on a : C est un multiple commun à A et à B. Mais alors $M|C$. D'où, $(A) \cap (B) = (C) \subset (M)$. Conclusion : $(A) \cap (B) = (M)$.

Réciproquement, si $(M) = (A) \cap (B)$, alors M est un multiple commun à A et à B, et, d'après la première partie de la démonstration, si P est un multiple commun à A et à B, alors $(P) \subset (A) \cap (B) = (M)$. D'où, P est un multiple de M.

Proposition 3.2.13 *Soient a et b des éléments de $\mathbb{K}[X]$ premiers entre eux.*
Alors, $(a) \cap (b) = (ab)$.

Cette proposition indique donc que lorsque deux éléments de $\mathbb{K}[X]$ sont premiers entre eux, leur produit est un PPCM.

Démonstration 3.2.13 Comme $ab \in (a)$ et $ab \in (b)$, on a $ab \in (a) \cap (b)$ et donc $(ab) \subset (a) \cap (b)$.
Montrons l'inclusion de $(a) \cap (b)$ dans (ab). Soit p un multiple commun à a et à b. On sait qu'alors $(p) \subset (a) \cap (b)$. Montrons que $(p) \subset (ab)$. Comme p est un multiple de a, il existe α dans $\mathbb{K}[X]$ tel que $p = \alpha a$. De même, il existe β tel que $p = \beta b$. De $\alpha a = \beta b$, on déduit que $a|\beta b$. Or, comme a et b sont premiers entre eux, le théorème de Gauss 3.2.11 implique que $a|\beta$. Donc, $\beta = qa$ pour un certain $q \in \mathbb{K}[X]$. D'où, $p = \beta b = qab$, et donc $(p) \subset (ab)$. Choisissons un multiple commun particulier : un PPCM de a et de b, et nous obtenons grâce au théorème 3.2.12 : $(a) \cap (b) \subset (ab)$.

Théorème 3.2.14 *Soient A, B, Δ et M dans $\mathbb{K}[X]$.*
Si $(A,B) = (\Delta)$ et $(A) \cap (B) = (M)$, alors il existe λ dans $\mathbb{K}^*$ tel que : $AB = \lambda \Delta M$.

La démonstration de ce théorème est assez longue. Elle repose sur des lemmes dont les résultats ont un intérêt en eux-mêmes.

Lemme 3.2.14.1 *Soient A, B, Δ, a et b des éléments de $\mathbb{K}[X]$ tels que :*
$(A,B) = (\Delta) \neq \{0\}$, $A = \Delta a$ et $B = \Delta b$.
Alors, a et b sont premiers entre eux.

Ce lemme indique que lorsqu'on divise deux polynômes non tous les deux nuls par un de leurs PGCD, on obtient deux polynômes premiers entre eux.

Démonstration 3.2.14.1 Soit $P \in \mathbb{K}[X]$. Supposons que $P|a$ et $P|b$. Alors, $\Delta P|A$ et $\Delta P|B$. Comme Δ est un PGCD de A et B, $\Delta P|\Delta$. Il existe donc $Q \in \mathbb{K}[X]$ tel que : $\Delta = \Delta PQ$. Comme $\Delta \neq 0$, $\deg(\Delta) \in \mathbb{N}$, alors de $\deg(\Delta) = \deg(\Delta) + \deg(P) + \deg(Q)$, on déduit : $\deg(P) = 0$, et donc : $P \in \mathbb{K}[X]^*$.

11. "Plus Petit Commun Multiple"

Lemme 3.2.14.2 *Soient A, B, Δ, a et b des éléments de $\mathbb{K}[X]$ tels que :*
$A = \Delta a$, $B = \Delta b$ et a et b sont sont premiers entre eux.
Alors, $(A) \cap (B) = (\Delta ab)$.

Démonstration 3.2.14.2 $\Delta ab = Ab = aB$, donc $\Delta ab \in (\Delta ab) \subset (A) \cap (B)$.
Montrons l'inclusion réciproque. Soit P un multiple commun à A et à B. Il existe α et β dans $\mathbb{K}[X]$ tels que : $P = \alpha A = \alpha \Delta a$ et $P = \beta B = \beta \Delta b$. On en déduit : $\Delta(\alpha a - \beta b) = 0$. comme $\mathbb{K}[X]$ est intègre, $\Delta(\alpha a - \beta b) = 0$ si et seulement si $\Delta = 0$ ou $\alpha a = \beta b$. Si $\Delta = 0$, alors $A = B = \Delta ab = 0$ et la conclusion du lemme est vérifiée. Si $\Delta \neq 0$, alors $\alpha a = \beta b$. Dans ce cas, $a|\alpha a = \beta b$. Comme $(a,b) = (1)$, le théorème 3.2.11 a pour conséquence : $a|\beta$. Il existe donc q dans $\mathbb{K}[X]$, tel que $\beta = qa$. Alors, $P = \Delta \beta b = q \Delta ab$ et donc $P \in (P) \subset (\Delta ab)$. Si nous choisissons un PPCM, cette dernière inclusion devient : $(P) = (A) \cap (B) \subset (\Delta ab)$.

Démonstration 3.2.14 Démonstration du théorème 3.2.14 : Si $\Delta = 0$, alors $A = B = 0$ et la conclusion du théorème est vraie. Supposons $\Delta \neq 0$. Posons $A = \Delta a$ et $B = \Delta b$. Alors, d'après le lemme 3.2.14.1, a et b sont premiers entre eux. D'après le lemme 3.2.14.2, Δab est un PPCM de A et de B. Soit M un PPCM de A et de B. D'après ce qui précède, on a : $(M) = (A) \cap (B) = (\Delta ab)$. Donc (proposition 3.2.7), il existe λ dans $\mathbb{K}^*$ tel que : $\Delta ab = \lambda M$. D'où, en multipliant chacun des membres de cette dernière égalité par Δ : $\lambda \Delta M = \Delta a \Delta b = AB$.

Théorème 3.2.15 *Soient A, B, Δ et M dans $\mathbb{K}[X]$, $\Delta \neq 0$.*
Si $(A,B) = (\Delta)$ et s'il existe λ dans $\mathbb{K}^*$ tel que $AB = \lambda \Delta M$, alors M est un PPCM de A et de B.

Ce dernier théorème est bien utile, si l'on dispose d'un PGCD, pour calculer un PPCM. En effet, si $(A,B) = (\Delta) \neq 0$, alors le quotient (le résultat) de la division de AB par Δ est un PPCM.

Démonstration 3.2.15 Notons C un PPCM de A et de B. D'après le théorème 3.2.14, il existe $\mu \in \mathbb{K}^*$ tel que $\mu \Delta C = AB$. Comme $\lambda \Delta M = AB$, on en déduit : $\Delta(\mu C - \lambda M) = 0$. Comme $\mathbb{K}[X]$ est intègre, cette dernière égalité entraîne $\Delta = 0$ ou $\mu C = \lambda M$. Puisque $\Delta \neq 0$, on a : $\mu C = \lambda M$. On en déduit : $C = \lambda \mu^{-1} M$, et comme $\lambda \mu^{-1} \in \mathbb{K}^*$, on a $(C) = (M)$ (proposition 3.2.7). Donc, d'après le théorème 3.2.12, M est un PPCM de A et de B.

Algorithme d'Euclide

L'algorithme d'Euclide permet d'obtenir un PGCD de deux polynômes par la méthode des divisions successives.

Exercice 3.2.8 *Soient A et B dans $\mathbb{K}[X]$.*
Montrer que :
1. *$(A,0) = (A)$.*
2. *Si $B|A$, alors $(A,B) = (B)$.*

Proposition 3.2.16 *Soit B un polynôme non nul et A un polynôme quelconque. Si Q et R sont respectivement, le quotient et le reste de la division euclidienne de A par B, alors : $(A,B) = (B,R)$.*

Démonstration 3.2.16 On a : $A = BQ + R$. Donc, $A \in (B,R)$. Comme $B \in (B,R)$, on obtient : $(A,B) \subset (B,R)$. De $R = A - BQ$, on déduit : $R \in (A,B)$. Comme $B \in (A,B)$, on a : $(B,R) \subset (A,B)$.

Cette proposition et les résultats de l'exercice 3.2.8 sont utilisés pour justifier l'algorithme d'Euclide.
Recherche d'un PGDC Δ de A et B. Description de l'algorithme :
* Si $A = 0$, alors $(A,B) = (B)$ et $\Delta = B$.
* Si $B = 0$, alors $(A,B) = (A)$ et $\Delta = A$.
* Si $A \neq 0$ et $B \neq 0$, posons $B_0 = A$ et $R_0 = B$.
  Définition par récurrence des B_n et des R_n :
  - Si $R_n = 0$, alors $\Delta = B_n$.
  - Si $R_n \neq 0$, alors $B_{n+1} = R_n$ et R_{n+1} est le reste de la division euclidienne de B_n par R_n.

D'après la proposition 3.2.16, $(A,B) = (B_n,R_n)$. D'où, si $R_n = 0$, alors, d'après l'exercice 3.2.8 $(A,B) = (B_n)$. D'autre part, on est assuré que l'algorithme s'arrête, car : $\deg(R_{n+1}) < \deg(R_n)$. Après un nombre fini d'étapes, on obtiendra forcément $\deg(R_n) < 0$ et donc $R_n = 0$.

3.3 Fonctions polynômiales

Définition et notation 3.3.1 *Soient $a \in \mathbb{K}$ et $P(X) \in \mathbb{K}[X]$ de degré n. Soit $\sum_{k=0}^{n} \lambda_k X^k$ (0, si $P = 0$) la forme canonique de $P(X)$. On définit l'élément $P(a)$ de $\mathbb{K}$ par : $P(a) = \sum_{k=0}^{n} \lambda_k a^k$ (0, si $P = 0$).*

Définition 3.3.2 (Fonction polynômiale) *Soit f une application de $\mathbb{K}$ dans $\mathbb{K}$. S'il existe un polynôme $P(X) \in \mathbb{K}[X]$ tel que, pour tout $a \in \mathbb{K}$, $f(a) = P(a)$, alors on dit que f est une fonction polynômiale (ou fonction polynôme).*

Exercice 3.3.1 *Montrer que pour tout a et tout λ dans $\mathbb{K}$, et pour tout P et tout Q dans $\mathbb{K}[X]$, on a :*

1. $(P+Q)(a) = P(a) + Q(a)$
2. $(PQ)(a) = P(a)Q(a)$
3. $(\lambda P)(a) = \lambda(P(a))$
4. *Si $P(X) = X^0$, alors $P(a) = 1$.*

Définition 3.3.3 (Racine) *On dit que $a \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$, lorsque $P(a) = 0$.*

Théorème 3.3.1 *Pour tout a dans $\mathbb{K}$ et tout P dans $\mathbb{K}[X]$: a est une racine de P, si et seulement si, $X - a | P$.*

Démonstration 3.3.1 On rappelle que $X - a$ est le polynôme anciennement noté : $X^1 - aX^0$. Supposons que a soit une racine de P. Comme $X - a \neq 0$, on peut effectuer la division euclidienne de P par $X - a$. Notons respectivement Q et R le quotient et le reste de la division euclidienne de P par $X - a$. On a : $P(X) = (X-a)Q(X) + R(X)$. Alors, $P(a) = (a-a)Q(a) + R(a) = 0 + R(a) = R(a) = 0$. Or, $\deg(R) < \deg(X - a) = 1$. Donc, $R(X) = \alpha X^0 = \alpha$ pour un certain α dans $\mathbb{K}$. De $R(a) = 0$, on déduit alors $R(X) = \alpha = 0$ et donc $P(X) = (X - a)Q(X)$.

Réciproquement, supposons $X - a | P$. Alors, il existe Q dans $\mathbb{K}[X]$ tel que $P(X) = (X - a)Q(X)$. D'où : $P(a) = (a - a)Q(a) = 0$.

3.4 Polynôme dérivé

Définition et notation 3.4.1 (Polynôme dérivé) *Soit P un polynôme de $\mathbb{K}[X]$. Supposons : $\deg(P) = n$. Soit $\sum_{k=0}^{n} \lambda_k X^k$ (0 si $P = 0$) la forme canonique de P. Le polynôme dérivé de P, noté P', est défini par :*

$$P'(X) = \begin{cases} 0 & si \ \deg(P) \leqslant 0 \\ \sum_{k=0}^{n-1} (k+1)\lambda_{k+1} X^k & si \ \deg(P) \geqslant 1 \end{cases}$$

Proposition 3.4.1 *Pour tout P et tout Q dans $\mathbb{K}[X]$, on a :*

1. $(P+Q)' = P' + Q'$
2. $(PQ)' = P'Q + PQ'$
3. $(\forall \lambda \in \mathbb{K}) \quad (\lambda P)' = \lambda P'$

Démonstration 3.4.1 La première et la dernière propriétés sont triviales. Pour la seconde, il suffit d'après les deux autres propriétés, de montrer que : $(X^n X^m)' = (X^n)' X^m + X^n (X^m)'$. D'après la définition du polynôme dérivé :

$$(X^n)' = \left(\sum_{k=0}^{+\infty} \delta_{nk} X^k \right)' = \sum_{k=0}^{+\infty} (k+1)\delta_{nk+1} X^k = \begin{cases} nX^{n-1} & \text{si } n \neq 0 \\ 0 & \text{si } n = 0 \end{cases}$$

En utilisant la convention : $0X^{-1} = 0$, on en déduit : $(X^n)' = nX^{n-1}$ pour tout n dans $\mathbb{N}$. Alors, $(X^n)' X^m + X^n (X^m)' = nX^{n-1}X^m + mX^n X^{m-1} = nX^{n+m-1} + mX^{n+m-1} = (n+m)X^{n+m-1} = (X^{n+m})'$.

3.5 Polynômes irréductibles

Définition 3.5.1 (Polynôme irréductible) *Soit P un élément de $\mathbb{K}[X]$. On dit que P est irréductible si :*

1. *$P \notin \mathbb{K}^*$, ce qui équivaut [12] à : $\deg(P) \neq 0$.*
2. *Pour tout $A \in \mathbb{K}[X]$ et tout $B \in \mathbb{K}[X]$, $P = AB$ implique $A \in \mathbb{K}^*$ ou $B \in \mathbb{K}^*$.*

12. Une fois encore, $\mathbb{K}^*$ est identifié à $\mathbb{K}[X]^*$.

Exemple important : Soit $a \in \mathbb{K}$. Le polynôme $X-a$ est irréductible. En effet, si pour $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$, $X-a=AB$, alors (théorème 3.1.2) $\deg(A)+\deg(B)=\deg(X-a)=1$. D'où, $\deg(A)=0$ ou $\deg(B)=0$, et donc A ou B est inversible.

Exercice 3.5.1 *Soit P un polynôme de $\mathbb{K}[X]$. Montrer que si P est irréductible, alors $P \neq 0$.*

Définition 3.5.2 (Polynôme unitaire) *Soit $P \in \mathbb{K}[X]$, $P \neq 0$. On dit que $P=\sum_{k=0}^{\deg(P)} \lambda_k X^k$ est unitaire lorsque $\lambda_{\deg(P)}=1$.*

Pour tout $a \in \mathbb{K}$, le polynôme $X-a$ est à la fois irréductible et unitaire.

Théorème 3.5.1 (Décomposition) *Tout polynôme non nul A de $\mathbb{K}[X]$ admet une unique (à l'ordre des facteurs près) décomposition en produit d'un élément de $\mathbb{K}^*$ et de facteurs irréductibles et unitaires.*

Ce théorème indique qu'à tout polynôme A de $\mathbb{K}[X]$, correspond un élément λ de $\mathbb{K}^*$, des polynômes irréductibles et unitaires : P_1, P_2,..., P_n, déterminés de manière unique, et tels que : $A=\lambda P_1 P_2 \cdots P_n$.

Démonstration 3.5.1 Montrons l'existence d'une décomposition, par récurrence sur le degré du polynôme A.
Si $\deg(A)=0$, alors $A=\lambda \in \mathbb{K}^*$ et la décomposition est $A=\lambda$.
Supposons que tout polynôme de degré inférieur ou égal à p soit le produit d'un élément de $\mathbb{K}^*$ et de polynômes irréductibles et unitaires. Montrons qu'alors, si $\deg(A)=p+1$, A possède également une décomposition en produit d'un élément de $\mathbb{K}^*$ par des polynômes irréductibles et unitaires.
Si $A=aX^{p+1}+\sum_{k=0}^{p} a_k X^k$ est irréductible, alors $A=a\left(a^{-1}A\right)$, avec $a \in \mathbb{K}^*$ et $a^{-1}A$ irréductible et unitaire.
Sinon, A n'est pas irréductible, et dans ce cas, il existe B et C dans $\mathbb{K}[X]$, non inversibles l'un comme l'autre, tels que : $A=BC$. Puisque $A \neq 0$, on a : $B \neq 0$ et $C \neq 0$. Comme ni B, ni C n'est inversible, on a : $\deg(B) \geqslant 1$ et $\deg(C) \geqslant 1$. D'où, comme $p+1=\deg(B)+\deg(C)$, $\deg(B) \leqslant p$ et $\deg(C) \leqslant p$. En appliquant l'hypothèse de récurrence à B et à C, on obtient que ces polynômes admettent une décomposition. Alors, le produit des décomposition respectives de B et de C fournit une décomposition pour A.

La démonstration de l'unicité de la décomposition est plus délicate, et utilisera les résultats des lemmes suivants :

Lemme 3.5.1.1 *Si P est un polynôme irréductible, alors, pour tout polynôme A : $(A,P)=(P)$ ou $(A,P)=\mathbb{K}[X]$.*

Démonstration 3.5.1.1 Comme $\mathbb{K}[X]$ est principal, il existe $D \in \mathbb{K}[X]$ tel que : $(A,P)=(D)$. Comme $P \in (A,P)=(D)$, il existe $Q \in \mathbb{K}[X]$ tel que : $P=QD$. Alors, puisque P est irréductible, Q ou D est inversible. Si Q est inversible, alors $(P)=(D)=(A,P)$. Si D est inversible, alors $(A,P)=\mathbb{K}[X]$.

Lemme 3.5.1.2 *Si P est irréductible, et si $P|AB$, alors $P|A$ ou $P|B$.*

Démonstration 3.5.1.2 Si P ne divise pas A, alors, d'après le lemme 3.5.1.1, $(A,P)=\mathbb{K}[X]$. Dans ce cas, il existe des polynômes U et V tel que : $AU+PV=1$. On en déduit : $B=ABU+PBV$. Mais alors, $P|B$ car $P|ABU$ et $P|PBV$.

Lemme 3.5.1.3 *Si P et Q sont irréductibles et unitaires, et si $P|Q$, alors $P=Q$.*

Démonstration 3.5.1.3 D'après le lemme 3.5.1.1, $(P,Q)=\mathbb{K}[X]$ ou $(P,Q)=(P)=(Q)$. Comme $P|Q$, alors $(P,Q)=(P)$ et donc, il existe $\lambda \in \mathbb{K}^*$ tel que $P=\lambda Q$. De cette dernière égalité, on déduit $\deg(P)=\deg(Q)$. D'après le théorème 3.1.3, comme $P=\lambda Q$ les monômes de degré $\deg(P)$ de P et de λQ doivent être identiques. Or, le monôme de degré $\deg(P)$ de P est $X^{\deg(P)}$, et celui de λQ est $\lambda X^{\deg(P)}$. D'où : $\lambda=1$.

Démonstration 3.5.1 (Fin de la démonstration du théorème 3.5.1). Montrons l'unicité de la décomposition de A, par récurrence sur le nombre maximal de facteurs irréductibles deux décompositions de A. Supposons $A=\lambda P_1 P_2 \cdots P_n = \mu Q_1 Q_2 \cdots Q_m$, où λ et μ sont dans $\mathbb{K}^*$, les polynômes P_i, ainsi que les Q_j, sont irréductibles et unitaires. La récurrence porte donc sur $k=\max\{n,m\}$.
Si $k=0$, alors $A=\lambda=\mu$ et les deux décompositions sont bien identiques.
Supposons la propriété d'identité des deux décompositions vérifiée pour des décompositions dont la plus "longue" comporte k facteurs irréductibles.
Supposons : $A=\lambda P_1 P_2 \cdots P_{k+1}=\mu Q_1 Q_2 \cdots Q_m$ avec $m \leqslant k+1$. Comme $P_{k+1}|\mu Q_1 Q_2 \cdots Q_m$, d'après le lemme 3.5.1.2, appliqué autant de fois que nécessaire, P_{k+1} divise un des Q_i. Quitte à indexer différemment les Q_i, supposons que $P_{k+1}|Q_m$. Alors, d'après le lemme 3.5.1.3, $P_{k+1}=Q_m$. Mais alors, de $A=\lambda P_1 P_2 \cdots P_{k+1}=\mu Q_1 Q_2 \cdots Q_m$, et

de $P_{k+1} = Q_m$, on déduit : $P_{k+1}(\lambda P_1 P_2 \cdots P_k - \mu Q_1 Q_2 \cdots Q_{m-1}) = 0$. Comme $\mathbb{K}[X]$ est intègre et $P_{k+1} \neq 0$, on a : $\lambda P_1 P_2 \cdots P_k = \mu Q_1 Q_2 \cdots Q_{m-1}$. Il ne reste plus qu'à utiliser l'hypothèse de récurrence sur les deux décompositions figurant dans cette dernière égalité.

Exercice 3.5.2 *Soient P et Q des polynômes irréductibles et unitaires. Montrer que $P = Q$ ou bien $(P,Q) = (1)$. (Indication : lire attentivement les démonstrations des lemmes 3.5.1.1 et 3.5.1.3).*

3.5.1 Polynômes irréductibles de $\mathbb{C}[X]$

Le théorème de D'Alembert sera admis. Les outils nécessaires à sa démonstration [13] ne sont pas à notre programme d'algèbre du premier semestre.

Théorème 3.5.2 (D'Alembert) *Tout polynôme de $\mathbb{C}[X]$ de degré supérieur ou égal à un admet une racine dans $\mathbb{C}$.*

Corollaire 3.5.2.1 *Soit $P \in \mathbb{C}[X]$.*
P est un polynôme irréductible et unitaire de $\mathbb{C}[X]$, si et seulement si, il existe $a \in \mathbb{C}$ tel que : $P = X - a$.

Démonstration 3.5.2.1 Nous savons déjà que $X - a$ est un polynôme irréductible et unitaire. Supposons P irréductible et unitaire. Dans ce cas, $\deg(P) \geqslant 1$. Appliquons à P le théorème de D'Alembert : P admet une racine dans $\mathbb{C}$. Notons a cette racine. D'après le théorème 3.3.1, $X - a | P$. Il existe donc $Q \in \mathbb{C}[X]$ tel que : $P = (X - a)Q$. Comme P est irréductible, ainsi que $X - a$, $Q = \lambda \in \mathbb{C}^*$. Comme P est unitaire : $\lambda = 1$.

Définition 3.5.3 (Racine d'ordre r) *Soient $P \in \mathbb{C}[X]$, $a \in \mathbb{C}$, et $r \in \mathbb{N} \setminus \{0\}$. On dit que a est une racine d'ordre r de P, s'il existe $Q \in \mathbb{C}[X]$ tel que : $P = (X - a)^r Q$ et $Q(a) \neq 0$. r est alors l'ordre de multiplicité de la racine a. Si $r > 1$, on dit que a est une racine multiple [14] de P.*

Le théorème 3.5.1 appliqué aux polynômes de $\mathbb{C}[X]$, nous donne : tout polynôme $P \in \mathbb{C}[X]$, de degré supérieur ou égal à zéro, se factorise [15] dans $\mathbb{C}[X]$ de la manière suivante :

$$P = \lambda \prod_{i=1}^{n} (X - a_i)^{r_i}$$

a_1, $a_2, \ldots$, a_n étant les n racines distinctes de P dans $\mathbb{C}$, de multiplicités respectives r_1, $r_2, \ldots$, r_n, et λ un élément de $\mathbb{C}^*$. Remarquons que $\deg(P) = \sum_{i=1}^{n} r_i$.

3.5.2 Polynômes irréductibles de $\mathbb{R}[X]$

Proposition 3.5.3 *Soient α et β dans $\mathbb{R}$. Si le discriminant $\Delta = \alpha^2 - 4\beta$ de $X^2 + \alpha X + \beta$ est strictement négatif, alors le polynôme $X^2 + \alpha X + \beta$ est un polynôme irréductible et unitaire de $\mathbb{R}[X]$.*

Démonstration 3.5.3 Supposons [16] que $X^2 + \alpha X + \beta$ ne soit pas irréductible. Soient A et B dans $\mathbb{R}[X] \setminus \mathbb{R}^*$, tel que : $X^2 + \alpha X + \beta = AB$. Alors $\deg(A) + \deg(B) = 2$, et comme ni A, ni B, n'est inversible : $\deg(A) = \deg(B) = 1$. Puisque AB est unitaire, il existe $a \in \mathbb{R}$ et $b \in \mathbb{R}$ tels que : $A = X - a$ et $B = X - b$. Mais alors, $AB = X^2 - (a + b)X + ab$ et le discriminant est : $\Delta = (a + b)^2 - 4ab = (a - b)^2$. Donc, $\Delta \geqslant 0$.

Définition et notation 3.5.4 *Soit $P = \sum_{k=0}^{n} \lambda_k X^k \in \mathbb{C}[X]$. On définit le conjugué $\bar{P}$ de P par : $\bar{P}(X) = \sum_{k=0}^{n} \bar{\lambda}_k X^k$.*

Exercice 3.5.3 *Soient P et Q dans $\mathbb{C}[X]$.*
Montrer que $\overline{P + Q} = \bar{P} + \bar{Q}$ et $\overline{PQ} = \bar{P}\bar{Q}$.

Proposition 3.5.4 *Soit $P \in \mathbb{R}[X]$. Si P admet le nombre complexe a pour racine d'ordre r, alors P admet aussi le nombre complexe $\bar{a}$ pour racine d'ordre r.*

13. Tout ouvrage honnête présentant les mathématiques d'un premier cycle universitaire scientifique, propose une démonstration du théorème de D'Alembert.
14. Par exemple, une racine double est une racine dont l'ordre de multiplicité est deux.
15. $\prod$ est la notation usuelle du produit. $\prod_{i=1}^{n} u_i = u_1 \times u_2 \times \cdots \times u_n$.
16. Le procédé de démonstration utilisé ici consiste à prouver la contraposée de la proposition énoncée ; c'est à dire, pour prouver "si $\mathcal{A}$ est vraie alors $\mathcal{B}$ est vraie", on prouve : "si $\mathcal{B}$ est fausse, alors $\mathcal{A}$ est fausse".

Démonstration 3.5.4 Puisque $P \in \mathbb{R}[X]$, considérons que P est un polynôme de $\mathbb{C}[X]$ dont les coefficients sont réels. Si a est une racine d'ordre r de P, alors il existe $Q \in \mathbb{C}[X]$ tel que : $P = (X-a)^r Q$ et $Q(a) \neq 0$. Comme $P \in \mathbb{R}[X]$, $P = \bar{P} = (X-\bar{a})^r \bar{Q}$. Comme $\bar{Q}(\bar{a}) = \overline{Q(a)}$ et $Q(a) \neq 0$, $\bar{a}$ est bien une racine d'ordre r de P.

Soit $P \in \mathbb{R}[X]$. Considéré comme polynôme de $\mathbb{C}[X]$, P admet pour décomposition :

$$P = \lambda \prod_{i=1}^{n} (X-a_i)^{r_i} = \lambda \prod_{\substack{i=1 \\ a_i \in \mathbb{R}}}^{n} (X-a_i)^{r_i} \prod_{\substack{i=1 \\ a_i \notin \mathbb{R}}}^{n} (X-a_i)^{r_i}$$

Remarquons, pour commencer, que $\lambda \in \mathbb{R}$. En effet, λ est le coefficient de $X^{\deg(P)}$ dans P qui est à coefficients réels. D'après la proposition 3.5.4, le produit $\prod_{\substack{i=1 \\ a_i \notin \mathbb{R}}}^{n} (X-a_i)^{r_i}$ est composé de facteurs de type : $(X-a_i)^{r_i}(X-\bar{a}_i)^{r_i}$.
Or, $(X-a_i)^{r_i}(X-\bar{a}_i)^{r_i} = (X^2 - 2\Re e(a_i) + |a_i|^2)^{r_i}$. Le discriminant du polynôme de $\mathbb{R}[X]$: $X^2 - 2\Re e(a_i) + |a_i|^2$, vaut $4((\Re e(a_i))^2 - |a_i|^2)$, qui est un nombre strictement négatif si $a_i \notin \mathbb{R}$. Donc, d'après la proposition 3.5.3, $X^2 - 2\Re e(a_i) + |a_i|^2$ est irréductible dans $\mathbb{R}[X]$.
Conclusion : tout polynôme non nul P de $\mathbb{R}[X]$, se factorise en produit de facteurs irréductibles dans $\mathbb{R}[X]$, de la manière suivante :

$$P = \lambda \prod_{i=1}^{n} (X-a_i)^{r_i} \prod_{j=1}^{m} (X^2 + \alpha_j X + \beta_j)^{s_j}$$

les a_i étant les racines de P dans $\mathbb{R}$, r_i l'ordre de multiplicité de la racine a_i, les polynômes $X^2 + \alpha_j X \beta_j$ ayant un discriminant strictement négatif, s_j étant le nombre de fois où le polynôme $X^2 + \alpha_j X + \beta_j$ apparaît dans le produit.

Chapitre 4

Algèbre linéaire

$\mathbb{K}$ désigne indifféremment $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

4.1 $\mathbb{K}$-espaces vectoriels

Définition et notation 4.1.1 *Soient $\mathcal{A}$ et $\mathcal{B}$ des ensembles. $\mathcal{A} \times \mathcal{B}$ est l'ensemble* [1] *des couples (a, b), avec $a \in \mathcal{A}$ et $b \in \mathcal{B}$.*

Définition 4.1.2 (Loi externe) *Soient $\mathcal{A}$ et $\mathcal{B}$ des ensembles non vides. Une loi externe sur $\mathcal{B}$, à domaine d'opérateur $\mathcal{A}$, est une application de $\mathcal{A} \times \mathcal{B}$ vers $\mathcal{B}$.*

Un telle loi a déjà été définie page 24, de $\mathbb{K} \times \mathbb{K}[X]$ vers $\mathbb{K}[X]$.

Définition 4.1.3 (Espace vectoriel) *Soit E un ensemble non vide muni d'une loi interne $\top$ et d'une loi externe $*$ à domaine d'opérateur $\mathbb{K}$.*
E est un $\mathbb{K}$-espace vectoriel, ou : espace vectoriel sur $\mathbb{K}$, si les lois $\top$ et $*$ vérifient :

1. *$\top$ est une somme et E muni de cette loi est un groupe commutatif ; c'est à dire :*
   (a) *$\top$ est associative*
   (b) *$\top$ est commutative*
   (c) *$\top$ admet un élément neutre appelé : le vecteur nul*
   (d) *tout élément de E admet un opposé pour la loi $\top$*
2. *Pour tout α et tout β dans $\mathbb{K}$, tout x et tout y dans E :*
   (a) $\alpha * (x \top y) = (\alpha * x) \top (\alpha * y)$
   (b) $(\alpha + \beta) * x = (\alpha * x) \top (\beta * x)$
   (c) $\alpha * (\beta * x) = (\alpha\beta) * x$
   (d) $1 * x = x$

Exercice 4.1.1 *Soit E un $\mathbb{K}$-espace vectoriel muni des lois $\top$ et $*$. On suppose que $\top$ et $*$ vérifient les axiomes de la définition 4.1.3. Notons 0_E le vecteur nul de E et, pour x dans E, notons $x^{\top}$ l'opposé de x pour la loi $\top$. Montrer que :*

1. *Pour tout x dans E : $0 * x = 0_E$*
2. *Pour tout α dans $\mathbb{K}$: $\alpha * 0_E = 0_E$*
3. *Pour tout x dans E : $x^{\top} = (-1) * x$*
4. *Pour tout x dans E et tout α dans $\mathbb{R}$:*
   $\alpha * x = 0_E$ implique $\alpha = 0$ ou $x = 0_E$

Notation 4.1.4 *Le vecteur nul* [2] *de l'espace vectoriel E est noté : 0_E.*

Définitions 4.1.5 (Scalaires, Vecteurs) *Soit E un $\mathbb{K}$-espace vectoriel.*
Les éléments de $\mathbb{K}$ sont appelés : scalaires.
Les éléments de E sont appelés : vecteurs.

1. C'est l'ensemble des applications ϕ de $2 = \{0, 1\}$ vers $\mathcal{A} \cup \mathcal{B}$ telles que : $\phi(0) \in \mathcal{A}$ et $\phi(1) \in \mathcal{B}$.
2. Bien que la notation proposée ici soit plutôt répandue, signalons que l'on trouve la notation $\overrightarrow{0}$ dans de nombreux ouvrages.

Pour une plus grande clarté, dans la définition 4.1.3, la somme sur E a été notée à l'aide du symbole $\top$. Dans la pratique, cette somme est tout simplement notée comme la somme dans $\mathbb{K}$: $+$. De même, $\alpha * x$ correspond au produit du vecteur x par le scalaire α, et se note αx. D'après la définition 4.1.3, $E = \{0_E\}$ est un espace vectoriel.

Définition 4.1.6 (Sous-espace vectoriel) *Soit E un espace vectoriel, et soit F un sous-ensemble non vide de E vérifiant :*

1. $(\forall x \in E)(\forall y \in E) \quad (x \in F \text{ et } y \in F) \Rightarrow (x + y) \in F$
2. $(\forall \lambda \in \mathbb{K})(\forall x \in E) \quad x \in F \Rightarrow \lambda x \in F$

F est alors un sous-espace vectoriel de E.

Exercice 4.1.2

1. *Montrer qu'un sous-espace vectoriel est un espace vectoriel.*
2. *Montrer que tout sous-espace vectoriel de E contient le vecteur nul de E.*

4.1.1 Familles de vecteurs

Une définition de "combinaison linéaire" a été donnée page 24. Cette définition convenait au cas alors exposé. Nous allons devoir reprendre cette définition, et l'adapter au cadre des espaces vectoriels.

Définition et notation 4.1.7 (Famille d'éléments) *Considérons les ensembles $\mathcal{A}$ et $\mathcal{B}$. Une famille d'éléments de $\mathcal{B}$, indexée par les éléments de $\mathcal{A}$ est une application ψ de $\mathcal{A}$ vers $\mathcal{B}$. On a pour habitude de noter, pour $a \in \mathcal{A}$, son image par ψ : $\psi(a)$. Ce même élément, considéré comme élément de $\mathcal{B}$ indexé par a, se note : ψ_a. La famille ψ d'éléments de $\mathcal{B}$ indexés par les éléments de $\mathcal{A}$, se note : $(\psi_a)_{a\in\mathcal{A}}$.*

Exercice 4.1.3 *Soit E un $\mathbb{K}$-espace vectoriel. Soit $(F_i)_{i\in I}$, $I \neq \emptyset$, une famille de sous-espaces vectoriels de E. Montrer que $F = \bigcap_{i\in I} F_i$ est un sous-espace vectoriel de E.*

Définition 4.1.8 (Famille presque nulle) *Soit I un ensemble. On dit que la famille $(\lambda_i)_{i\in I}$ d'éléments de $\mathbb{K}$ est presque nulle s'il existe un sous-ensemble fini de I : $\mathcal{F}$, tel que $\lambda_i = 0$ pour tout $i \in I \setminus \mathcal{F}$.*

Notation 4.1.9 *La notation $\mathbb{K}^{(I)}$ désigne l'ensemble [3] des familles presque nulles d'éléments de $\mathbb{K}$, indexées par les éléments de I.*

Définition 4.1.10 (Combinaison linéaire) *Soit E un $\mathbb{K}$-espace vectoriel. Soit I un ensemble. Soient $(x_i)_{i\in I}$ une famille [4] de vecteurs de E, et $(\lambda_i)_{i\in I}$ une famille presque nulle d'éléments de $\mathbb{K}$.*
Alors, $\sum_{i\in I} \lambda_i x_i$ est une combinaison linéaire de la famille $(x_i)_{i\in I}$. (On dit aussi : combinaison linéaire des x_i).

Remarque : la somme figurant dans la définition 4.1.10 comporte un nombre fini de termes non nuls, car la famille $(\lambda_i)_{i\in I}$ est presque nulle. La définition 3.1.16 est un cas particulier de la définition 4.1.10, avec $E = \mathbb{K}[X]$ et $I = \mathbb{N}$.

Proposition 4.1.1 *Soit E un $\mathbb{K}$-espace vectoriel. Soit $(x_i)_{i\in I}$ une famille de vecteurs de E. L'ensemble des combinaisons linéaires de la famille $(x_i)_{i\in I}$ est le plus petit sous-espace vectoriel de E contenant tous les x_i, pour $i \in I$.*

Démonstration 4.1.1 (Remarque : si $I = \emptyset$ alors le sous-espace engendré par les combinaisons linéaires de la famille vide est $\{0_E\}$, car tout sous-espace vectoriel de E doit contenir 0_E). Montrons que l'ensemble C des combinaisons linéaires de la famille $(x_i)_{i\in I}$ est un sous-espace vectoriel de E. Soient x et y des éléments de C, soit $\lambda \in \mathbb{K}$. D'après la définition de C, il existe $(\lambda_i)_{i\in I}$ et $(\mu_i)_{i\in I}$, suites presque nulles d'éléments de $\mathbb{K}$, telles que $x = \sum_{i\in I} \lambda_i x_i$ et $y = \sum_{i\in I} \mu_i x_i$. Mais alors, $x + y = \sum_{i\in I}(\lambda_i + \mu_i)x_i \in C$, et $\lambda x = \sum_{i\in I}(\lambda\lambda_i)x_i \in C$.

Soit F est un sous-espace vectoriel de E tel que $x_i \in F$ pour tout $i \in I$. Montrons qu'alors $C \subset F$. Soit λ_i un élément de $\mathbb{K}$. Comme $x_i \in F$, on a : $\lambda_i x_i \in F$. Donc, si le sous-espace vectoriel F contient tous les x_i, $i \in I$, il contient chacun des termes d'une combinaisons linéaire $\sum_{i\in I} \lambda_i x_i$. Puisque les termes non nuls d'une combinaison linéaire sont en nombre fini, il suffit pour conclure, de montrer que pour tout $n \in \mathbb{N}$: si y_0, $y_1, \ldots,$ y_n sont des éléments de F, alors $\sum_{k=0}^{n} y_k \in F$. (démonstration par récurrence sur n à terminer).

3. On aurait pu noter : $\mathbb{K}^{(\mathbb{N})}$, l'ensemble des suites presque nulles d'éléments de $\mathbb{K}$, puis adopter après le théorème 3.1.3 la notation $\mathbb{K}[X]$ pour cet ensemble.

4. On rencontre souvent, à la place de "famille de vecteurs", les termes : "système de vecteurs". Cette dénomination sera parfois utilisée dans ce cours.

Définition et notation 4.1.11 (Sous-espace engendré) *Soit E un $\mathbb{K}$-espace vectoriel. Soit $A \subset E$. L'ensemble des combinaisons linéaires des éléments de A est le sous-espace vectoriel engendré par A. Ce sous-espace est noté :* $\mathrm{Vect}_{\mathbb{K}} A$ *(ou, plus simplement* $\mathrm{Vect} A$*).*

Définition 4.1.12 (Famille libre) *Soit E un $\mathbb{K}$-espace vectoriel. Soit $(x_i)_{i\in I}$ une famille de vecteurs de E. On dit que la famille $(x_i)_{i\in I}$ est libre, si :*

$$\left(\forall (\lambda_i)_{i\in I} \in \mathbb{K}^{(I)}\right) \quad \sum_{i\in I} \lambda_i x_i = 0_E \Rightarrow (\forall i \in I) \quad \lambda_i = 0$$

On retiendra que lorsque la famille $(x_i)_{i\in I}$ est libre, la seule façon d'obtenir le vecteur nul de E par combinaison linéaire des éléments de la famille, est d'écrire la combinaison linéaire triviale : $\sum_{i\in I} 0x_i$.
Remarque : la famille vide est libre.

Définition 4.1.13 (Vecteurs linéairement indépendants) *On dit que les vecteurs x_i, $i \in I$, du $\mathbb{K}$-espace vectoriel E sont linéairement indépendants, lorsque la famille $(x_i)_{i\in I}$ est libre.*

Définition 4.1.14 (Famille liée) *Toute famille de vecteurs qui n'est pas libre est liée.*

Exercice 4.1.4 *On considère le $\mathbb{R}$-espace vectoriel* [5] *$\mathbb{R}^2$.*
Montrer que la famille $((1,0),(0,1))$ est libre.

Une fois encore, l'usage simplifie les formulations. On remplace souvent "la famille $(x_i)_{i\in I}$ est libre", par : "les vecteurs x_i sont libres".

Exercice 4.1.5 *Soit $(x_i)_{i\in I}$ une famille libre de vecteurs de E.*
Soient $(\lambda_i)_{i\in I}$ et $(\mu_i)_{i\in I}$ dans $\mathbb{K}^{(I)}$.
Montrer que : $\sum_{i\in I} \lambda_i x_i = \sum_{i\in I} \mu_i x_i \iff (\forall i \in I) \quad \lambda_i = \mu_i$.

Proposition 4.1.2 *Soit $(x_i)_{i\in I}$ une famille libre de vecteurs de E.*
Pour tout un sous-ensemble J de I, la famille $(x_i)_{i\in J}$ est libre.

Démonstration 4.1.2 Si $J = \emptyset$, alors $(x_i)_{i\in J}$ est libre. Si $J \neq \emptyset$, supposons $(x_i)_{i\in J}$ liée. Il existerait alors une combinaison linéaire des x_i, $i \in J$, dont les coefficients ne seraient pas tous nuls, égale au vecteur nul. Mais alors cette combinaison serait une combinaison des x_i, $i \in I$ qui contredirait le fait que la famille $(x_i)_{i\in I}$ est libre.

Définition 4.1.15 (Famille génératrice) *Soit E un $\mathbb{K}$-espace vectoriel.*
Soit $(x_i)_{i\in I}$ une famille de vecteurs de E.
On dit que la famille $(x_i)_{i\in I}$ est génératrice, si $\mathrm{Vect}\,(x_i)_{i\in I} = E$; c'est à dire : tout vecteur de E est une combinaison linéaire des x_i.

Remarque : Si $I = \emptyset$, alors $(x_i)_{i\in I}$ est génératrice de $E = \{0_E\}$.

Définition 4.1.16 (Base) *Soit E un $\mathbb{K}$-espace vectoriel.*
Soit $(x_i)_{i\in I}$ une famille de vecteurs de E.
On dit que la famille $(x_i)_{i\in I}$ est une base de E, si $(x_i)_{i\in I}$ est à la fois libre et génératrice.

Par exemple, les vecteurs $(1,0)$ et $(1,1)$ forment une base de $\mathbb{R}^2$. En effet, pour tout vecteur (x,y), il existe une et une seule combinaison linéaire de $(1,0)$ et $(1,1)$ égale à (x,y) : $(x,y) = (x-y)(1,0) + y(1,1)$.
Notons que si $E = \{0_E\}$, alors E a pour base la famille vide.

Exercice 4.1.6 *Montrer que la famille $(X^n)_{n\in\mathbb{N}}$ est une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}[X]$.*

Définition 4.1.17 (Coordonnées) *Soit E un $\mathbb{K}$-espace vectoriel. Soit $(e_i)_{i\in I}$ base de E. Pour tout $x \in E$, il existe une unique combinaison linéaire des e_i égale à x : $\sum_{i\in I} \lambda_i e_i = x$. La famille presque nulle $(\lambda_i)_{i\in I}$ constitue alors les coordonnées de x dans la base $(e_i)_{i\in I}$.*

5. $(x,y) + (x',y') = (x+x', y+y')$ et $\lambda(x,y) = (\lambda x, \lambda y)$

4.1.2 Applications linéaires

Définition 4.1.18 (Application linéaire) *Soient E et F des $\mathbb{K}$-espaces vectoriels. On dit que $f : E \to F$ est linéaire* [6] *si, pour tout x et tout y dans E, et pour tout λ dans $\mathbb{K}$:*
$f(x+y) = f(x) + f(y)$ *et* $f(\lambda x) = \lambda f(x)$.

Exercice 4.1.7 *Soient E et F des espaces vectoriels sur $\mathbb{K}$, et f une application linéaire de E dans F.*
Montrer que :

1. $\mathrm{Im}f = \{y \in F \mid (\exists x \in E) \quad f(x) = y\}$ *est un sous-espace vectoriel de F.*
2. $\mathrm{Ker}f = \{x \in E \mid f(x) = 0_F\}$ *est un sous-espace vectoriel de E.*

Définitions et notations 4.1.19 (Image, Noyau) *Les sous-espaces vectoriels* $\mathrm{Im}f$ *et* $\mathrm{Ker}f$ *de l'exercice 4.1.7 sont respectivement l'image et le noyau de f.*

Exercice 4.1.8 *Montrer que $f : \mathbb{R}^2 \to \mathbb{R}$, définie par : $(x, y) \mapsto 2y - x$, est une application linéaire (d'espaces vectoriels sur $\mathbb{R}$) ; puis, déterminer l'image et le noyau de f.*

Proposition 4.1.3 *On considère les espaces vectoriels sur $\mathbb{K}$: E et F. Soit $(e_i)_{i\in I}$ une famille génératrice de E. Soit $f : E \to F$ une application linéaire.*
Alors, $\mathrm{Im}f = \mathrm{Vect}\,(f(e_i))_{i\in I}$.

Démonstration 4.1.3 Par définition, pour tout $i \in I$, $f(e_i) \in \mathrm{Im}f$. Comme $\mathrm{Im}f$ est un sous-espace vectoriel de F, et que $\mathrm{Vect}\,(f(e_i))_{i\in I}$ est le plus petit sous-espace de F contenant tous les $f(e_i)$, on a : $\mathrm{Vect}\,(f(e_i))_{i\in I} \subset \mathrm{Im}f$.
Soit $y \in \mathrm{Im}f$. Il existe x dans E, tel que $f(x) = y$. Comme $(e_i)_{i\in I}$ est une famille génératrice de E, il existe au moins une combinaison linéaire des e_i égale à x : $x = \sum_{k=0}^{n} \lambda_k e_{i_k}$. Alors, comme f est linéaire : $y = f(x) = \sum_{k=0}^{n} \lambda_k f(e_{i_k})$, et donc $y \in \mathrm{Vect}\,(f(e_i))_{i\in I}$. On en déduit : $\mathrm{Im}f \subset \mathrm{Vect}\,(f(e_i))_{i\in I}$

Définitions et notations 4.1.20 (n-uplet, composante) *Soit n un nombre entier naturel non nul, et soit E un espace vectoriel.*
La notation : E^n désigne l'ensemble des n-uplets d'éléments de E. $x \in E^n$ signifie : $x = (x_1,x_2,\ldots,x_n)$ avec $x_1,x_2,\ldots,x_n$ éléments de E. x_i est la i-ème composante du n-uplet $(x_1,\ldots,x_i,\ldots,x_n)$.

Exercice 4.1.9 *Soit E un $\mathbb{K}$-espace vectoriel.*
On définit sur E^n la somme par :
$(x_1,x_2,\ldots,x_n) + (y_1,y_2,\ldots,y_n) = (x_1 + y_1,x_2 + y_2,\ldots,x_n + y_n)$.
On définit le produit par les scalaires par :
$\lambda(x_1,x_2,\ldots,x_n) = (\lambda x_1,\lambda x_2,\ldots,\lambda x_n)$.
Montrer qu'alors, E^n est un $\mathbb{K}$-espace vectoriel.

$\mathbb{K}$ muni de ses lois usuelles + et $\times$, est un $\mathbb{K}$-espace vectoriel. Une façon simple de fabriquer des $\mathbb{K}$-espaces vectoriels à partir de $\mathbb{K}$, est de procéder comme dans l'exercice 4.1.9. Vous retrouverez dans bon nombre d'exercices des TD, les espaces vectoriels $\mathbb{R}^n$ et $\mathbb{C}^n$.

4.2 Formes n-linéaires alternées

4.2.1 Formes n-linéaires

Définition 4.2.1 (Forme n-linéaire) *Soit E un $\mathbb{K}$-espace vectoriel.*
Soit $f : E^n \to \mathbb{K}$ vérifiant, pour tout $(x_1,x_2,\ldots,x_n) \in E^n$, tout $y \in E$, tout $i \in [\![1,n]\!]$, et tout $\lambda \in \mathbb{K}$:

1. $f(x_1,\ldots,\underset{\substack{i-ème\\composante}}{x_i + y},\ldots,x_n) = f(x_1,\ldots,\underset{\substack{i-ème\\comp.}}{x_i},\ldots,x_n) + f(x_1,\ldots,\underset{\substack{i-ème\\comp.}}{y},\ldots,x_n)$
2. $f(x_1,\ldots,\underset{\substack{i-ème\\composante}}{\lambda x_i},\ldots,x_n) = \lambda f(x_1,\ldots,\underset{\substack{i-ème\\comp.}}{x_i},\ldots,x_n)$

On dit alors que f est une forme n-linéaire sur E.

6. On dit parfois, pour préciser : application $\mathbb{K}$-linéaire.

Une forme n-linéaire f est donc une application linéaire par rapport à chaque composante, et à valeurs dans $\mathbb{K}$.
Fixons un n-uplet de vecteurs de E : $(x_1,\ldots,x_n)$. Alors pour tout $i \in [\![1,n]\!]$, les applications $\psi_i : E \to \mathbb{K}$ définies par : $\psi_i(y) = f(x_1,\ldots,x_{i-1},y,x_{i+1},\ldots,x_n)$, sont linéaires.
Une forme 1-linéaire est une application linéaire à valeurs dans $\mathbb{K}$.

Exercice 4.2.1 *Soit f une forme n-linéaire sur l'espace vectoriel E. Montrer que $f(x_1,x_2,\ldots,x_n) = 0$ dès qu'il existe $i \in [\![1,n]\!]$ tel que $x_i = 0_E$.*

Définition 4.2.2 (Forme n-linéaire alternée) *Soit E un $\mathbb{K}$-espace vectoriel, et f une forme n-linéaire sur E.*
On dit que f est alternée si $f(x_1,\ldots,x_n) = 0$ dès que $x_i = x_j$ pour i et j dans $[\![1,n]\!]$, $i \neq j$.

Définition 4.2.3 (Forme n-linéaire antisymétrique) *Soit E un $\mathbb{K}$-espace vectoriel, et f une forme n-linéaire sur E.*
On dit que f est antisymétrique si, pour tout $(x_1,\ldots,x_n) \in E^n$:
$f(x_1,\ldots,\underset{i-\text{ème comp.}}{x_i},\ldots,\underset{j}{x_j},\ldots,x_n) = -f(x_1,\ldots,\underset{i}{x_j},\ldots,\underset{j}{x_i},\ldots,x_n)$.

Proposition 4.2.1 *Soit E un $\mathbb{K}$-espace vectoriel, et f une forme n-linéaire sur E. f est alternée si [7] et seulement si f est antisymétrique.*

Démonstration 4.2.1 Supposons f alternée.
Alors, $f(\ldots,\underset{i}{x_i + x_j},\ldots,\underset{j}{x_i + x_j},\ldots) = 0$.
Par multilinéarité :

$$\begin{aligned} f(\ldots,\underset{i}{x_i + x_j},\ldots,\underset{j}{x_i + x_j},\ldots) =& f(\ldots,\underset{i}{x_i},\ldots,\underset{j}{x_i + x_j},\ldots) \\ &+ f(\ldots,\underset{i}{x_j},\ldots,\underset{j}{x_i + x_j},\ldots) \\ =& f(\ldots,\underset{i}{x_i},\ldots,\underset{j}{x_i},\ldots) + f(\ldots,\underset{i}{x_i},\ldots,\underset{j}{x_j},\ldots) \\ &+ f(\ldots,\underset{i}{x_j},\ldots,\underset{j}{x_i},\ldots) + f(\ldots,\underset{i}{x_j},\ldots,\underset{j}{x_j},\ldots) \end{aligned}$$

Puisque f est alternée : $f(\ldots,\underset{i}{x_i},\ldots,\underset{j}{x_i},\ldots) = f(\ldots,\underset{i}{x_j},\ldots,\underset{j}{x_j},\ldots) = 0$.
D'où, $f(\ldots,\underset{i}{x_i},\ldots,\underset{j}{x_j},\ldots) + f(\ldots,\underset{i}{x_j},\ldots,\underset{j}{x_i},\ldots) = 0$.
Supposons f antisymétrique.
Alors, $f(\ldots,\underset{i}{x_i},\ldots,\underset{j}{x_j},\ldots) = -f(\ldots,\underset{i}{x_j},\ldots,\underset{j}{x_i},\ldots)$. D'où, si $x_i = x_j$, on a : $2f(\ldots,\underset{i}{x_i},\ldots,\underset{j}{x_i},\ldots) = 0$.

Exercice 4.2.2 *Soit $f : E^n \to \mathbb{K}$ n-linéaire alternée.*
Montrer que, pour tout $i \in [\![1,n]\!]$, et tout n-uplet $(x_1,\ldots,x_n) \in E^n$:
$f(x_1,\ldots,x_i,\ldots,x_n) = (-1)^{i+1} f(x_i,x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)$
(Indication : faire une récurrence sur $i \in [\![1,n]\!]$.)

Notons que si f est une forme n-linéaire alternée sur E, si $e = (e_1,e_2,\ldots,e_n)$ est une base de E, et si $(x_1,x_2,\ldots,x_n)$ est une famille de vecteurs de E, alors $f(x_1,x_2,\ldots,x_n) = \lambda f(e_1,e_2,\ldots,e_n)$, avec $\lambda \in \mathbb{K}$. En effet, en utilisant la multilinéarité de f, on obtient que $f(x_1,\ldots,x_n)$ est une somme de termes de type : $\alpha_{i_1 i_2 \cdots i_n} f(e_{i_1},e_{i_2},\ldots,e_{i_n})$, avec $\alpha_{i_1 i_2 \cdots i_n} \in \mathbb{K}$ et $(i_1,i_2,\ldots,i_n) \in [\![1,n]\!]^n$. Or, si pour r et s dans $[\![1,n]\!]$, $r \neq s$, on a : $e_{i_r} = e_{i_s}$, alors $f(e_{i_1},e_{i_2},\ldots,e_{i_n}) = 0$, car f est alternée. Les autres termes sont donc de type $\alpha_{i_1 i_2 \cdots i_n} f(e_{i_1},e_{i_2},\ldots,e_{i_n})$, avec pour tout r et tout s dans $[\![1,n]\!]$, $r \neq s \Rightarrow e_{i_r} \neq e_{i_s}$; autrement dit : chaque vecteur de la base e figure une et une seule fois dans $(e_{i_1},e_{i_2},\ldots,e_{i_n})$. D'où, comme f est alternée, il existe $\beta_{i_1 i_2 \cdots i_n} \in \mathbb{K}$ tel que : $\alpha_{i_1 i_2 \cdots i_n} f(e_{i_1},e_{i_2},\ldots,e_{i_n}) = \beta_{i_1 i_2 \cdots i_n} f(e_1,e_2,\ldots,e_n)$. De plus (voir l'exercice 4.2.2, $\beta_{i_1 i_2 \cdots i_n} = \alpha_{i_1 i_2 \cdots i_n}$ ou bien $\beta_{i_1 i_2 \cdots i_n} = -\alpha_{i_1 i_2 \cdots i_n}$.

Conclusion : Si $e = (e_1,e_2,\ldots,e_n)$ est une base de E, alors pour tout n-uplet $(x_1,x_2,\ldots,x_n)$ d'éléments de E, il existe un élément λ de $\mathbb{K}$, tel que, pour toute forme n-linéaire alternée f sur E :

$$f(x_1,x_2,\ldots,x_n) = \lambda f(e_1,e_2,\ldots,e_n)$$

(λ égal à la somme des coefficients $\beta_{i_1 i_2 \cdots i_n}$).

7. Lorsque vos explorations du monde des mathématiques vous conduiront à la découverte des corps de caractéristique 2, vous aurez alors des formes n-linéaires antisymétriques qui ne sont pas alternées... mais ceci est une autre histoire.

4.2.2 Formes n-linéaires alternées et familles de vecteurs

Proposition 4.2.2 *Soient E un $\mathbb{K}$-espace vectoriel, et f une forme n-linéaire alternée sur E.*
Si $(x_1,x_2,\dots,x_n)$ est une famille liée, alors $f(x_1,x_2,\dots,x_n)=0$.

Démonstration 4.2.2 Si la famille $(x_1,x_2,\dots,x_n)$ est liée, il existe une combinaison linéaire non triviale des x_i égale au vecteur nul ; c'est à dire : $\sum_{k\in[\![1,\,n]\!]}\lambda_k x_k=0_E$, et $\lambda_k\neq 0$ pour au moins un entier $k\in[\![1,n]\!]$. Soit $i_0\in[\![1,n]\!]$ tel que $\lambda_{i_0}\neq 0$. Alors, $x_{i_0}=\sum_{k\in[\![1,\,n]\!]\setminus\{i_0\}}-\frac{\lambda_k}{\lambda_{i_0}}x_k$. D'où, en utilisant la linéarité de f par rapport à sa i_0-ème variable :

$$f(x_1,\dots,x_n)=\sum_{k\in[\![1,\,n]\!]\setminus\{i_0\}}-\frac{\lambda_k}{\lambda_{i_0}}f(x_1,\dots,\underbrace{x_k}_{\substack{i_0-ème\\composante}},\dots,x_n).$$

Or, si $k\in[\![1,n]\!]\setminus\{i_0\}$, alors $f(x_1,\dots,\underbrace{x_k}_{\substack{i_0-ème\\composante}},\dots,x_n)=0$, car x_k figure deux fois dans le n-uplet. On en déduit la proposition.

Théorème 4.2.3 *Soient n un nombre entier naturel strictement positif, E un espace vectoriel et $(x_1,x_2,\dots,x_n)\in E^n$.*
Si la famille $(x_1,x_2,\dots,x_n)$ est libre, alors il existe une unique forme n-linéaire alternée f définie sur $(\mathrm{Vect}(x_1,x_2,\dots,x_n))^n$, telle que : $f(x_1,x_2,\dots,x_n)=1$.

Lemme 4.2.3.1 *Soit $(x_1,x_2,\dots,x_n)$ une famille libre de vecteurs de E.*
Soient $y_1,y_2,\dots,y_n$ des vecteurs de $\mathrm{Vect}(x_1,x_2,\dots,x_n)$.
Pour tout $j\in[\![1,n]\!]$, il existe un unique[8] *$\lambda_j\in\mathbb{K}$, il existe un unique $a_j\in\mathrm{Vect}(x_2,\dots,x_n)$, tels que : $y_j=\lambda_j x_1+a_j$.*

Démonstration 4.2.3.1 Comme, pour tout $j\in[\![1,n]\!]$, $y_j\in\mathrm{Vect}(x_1,x_2,\dots,x_n)$ et comme la famille $(x_1,x_2,\dots,x_n)$ est libre, il existe une unique combinaison linéaire : $\sum_{i=1}^n\alpha_{i\,j}x_i$ égale à y_j. D'où, l'existence et l'unicité de $\lambda_j=\alpha_{1\,j}$ et de $a_j=\sum_{i=2}^n\alpha_{i\,j}x_i$.

Démonstration 4.2.3 Montrons le théorème par récurrence sur le nombre de vecteurs dans la famille libre.
Pour $n=1$, (x_1) est libre si et seulement si $x_1\neq 0_E$. $\mathrm{Vect}(x_1)=\{\lambda x_1\mid\lambda\in\mathbb{K}\}$. La forme 1-linéaire alternée $f:\mathrm{Vect}(x_1)\to\mathbb{K}$ qui à λx_1 associe λ est l'unique forme 1-linéaire qui convienne.
Hypothèse de récurrence : pour l'entier n, $n\geqslant 2$, il existe une unique forme $n-1$-linéaire alternée g : $(\mathrm{Vect}(x_2,\dots,x_n))^{n-1}\to\mathbb{K}$ telle que $g(x_2,\dots,x_n)=1$. (On rappelle que si $(x_1,x_2,\dots,x_n)$ est libre, alors $(x_2,\dots,x_n)$ est libre.)
Soient $y_1,y_2,\dots,y_n$ des vecteurs de $\mathrm{Vect}(x_1,x_2,\dots,x_n)$. En reprenant les notations du lemme, posons $f(y_1,y_2,\dots,y_n)=\sum_{j=1}^n(-1)^{j+1}\lambda_j g(a_1,\dots,\overset{\wedge}{a_j},\dots,a_n)$, où $(a_1,\dots,\overset{\wedge}{a_j},\dots,a_n)$ est le $n-1$-uplet construit en retirant la j-ème composante du n-uplet $(a_1,a_2,\dots,a_n)$.
Prouvons que f ainsi définie est n-linéaire alternée.
La n-linéarité est assez facile à démontrer, et la rédaction de ce point est laissée en exercice.
Il est plus délicat de prouver que f est alternée.
Considérons le n-uplet $(y_1,\dots,y_n)$ d'éléments de $\mathrm{Vect}(x_1,x_2,\dots,x_n)$, tel que $y_{j_0}=y_{j_1}$ pour j_0 et j_1 distincts dans $[\![1,n]\!]$. On a alors : $y_{j_0}=y_{j_1}=\lambda_{j_0}x_1+a_{j_0}$, et donc $\lambda_{j_0}=\lambda_{j_1}$ et $a_{j_0}=a_{j_1}$.
Pour $j\in[\![1,n]\!]$, si $j\neq j_0$ et $j\neq j_1$, alors a_{j_0} figure deux fois dans le $n-1$-uplet $(a_1,\dots,\overset{\wedge}{a_j},\dots,a_n)$, et comme g est alternée : $g(a_1,\dots,\overset{\wedge}{a_j},\dots,a_n)=0$.
La somme définissant $f(y_1,y_2,\dots,y_n)$ se simplifie donc :

$$\begin{aligned}f(y_1,y_2,\dots,y_n)&=\sum_{j=1}^n(-1)^{j+1}\lambda_j g(a_1,\dots,\overset{\wedge}{a_j},\dots,a_n)\\&=(-1)^{j_0+1}\lambda_{j_0}g(a_1,\dots,\overset{\wedge}{a_{j_0}},\dots,a_n)+(-1)^{j_1+1}\lambda_{j_1}g(a_1,\dots,\overset{\wedge}{a_{j_1}},\dots,a_n)\\&=(-1)^{j_0+1}\lambda_{j_0}g(a_1,\dots,\overset{\wedge}{a_{j_0}},\dots,a_n)+(-1)^{j_1+1}\lambda_{j_0}g(a_1,\dots,\overset{\wedge}{a_{j_1}},\dots,a_n)\end{aligned}$$

8. Il existe un unique a dans $\mathcal{A}$ se note : $\exists!a\in\mathcal{A}$.

Montrons que la somme de ces deux termes est nulle.
Supposons $j_0 < j_1$ (on les choisit ainsi dès le départ).

$$\begin{aligned}
&g(a_1,\dots,a_{j_0},\dots,\overset{\wedge}{a_{j_1}},\dots,a_n)\\
&\quad = (-1)^{j_0+1} g(a_{j_0},a_1,\dots,a_{j_0-1},a_{j_0+1},\dots,a_{j_1-1},a_{j_1+1},\dots,a_n)\\
&g(a_1,\dots,\overset{\wedge}{a_{j_0}},\dots,a_{j_1},\dots,a_n)\\
&\quad = (-1)^{j_1} g(a_{j_1},a_1,\dots,a_{j_0-1},a_{j_0+1},\dots,a_{j_1-1},a_{j_1+1},\dots,a_n)\\
&\quad = (-1)^{j_1} g(a_{j_0},a_1,\dots,a_{j_0-1},a_{j_0+1},\dots,a_{j_1-1},a_{j_1+1},\dots,a_n)
\end{aligned}$$

D'où,

$$\begin{aligned}
&f(y_1,y_2,\dots,y_n)\\
&\quad = (-1)^{j_0+1}\lambda_{j_0} g(a_1,\dots,\overset{\wedge}{a_{j_0}},\dots,a_n) + (-1)^{j_1+1}\lambda_{j_0} g(a_1,\dots,\overset{\wedge}{a_{j_1}},\dots,a_n)\\
&\quad = \lambda_{j_0}((-1)^{j_0+1}(-1)^{j_1} g(a_{j_0},a_1,\dots,a_{j_0-1},a_{j_0+1},\dots,a_{j_1-1},a_{j_1+1},\dots,a_n)\\
&\qquad +(-1)^{j_1+1}(-1)^{j_0+1} g(a_{j_0},a_1,\dots,a_{j_0-1},a_{j_0+1},\dots,a_{j_1-1},a_{j_1+1},\dots,a_n))\\
&\quad = (1-1)\lambda_{j_0}((-1)^{j_0+j_1+1} g(a_{j_0},a_1,\dots,a_{j_0-1},a_{j_0+1},\dots,a_{j_1-1},a_{j_1+1},\dots,a_n))\\
&\quad = 0
\end{aligned}$$

Donc, f est alternée.
D'après la définition de f, $f(x_1,x_2,\dots,x_n) = 1 g(x_2,\dots,x_n) = 1$.
Pour montrer l'unicité de f, supposons qu'il existe une forme n-linéaire alternée ψ sur $\mathrm{Vect}(x_1,\dots,x_n)$, telle que $\psi(x_1,x_2,\dots,x_n) = 1$, et montrons qu'alors $f = \psi$.
Soit $(y_1,y_2,\dots,y_n) \in (\mathrm{Vect}(x_1,x_2,\dots,x_n))^n$. Pour chaque y_j, $j \in [\![1,n]\!]$, il existe une unique combinaison linéaire : $\sum_{i=1}^n \alpha_{i\,j} x_i$, égale à y_j, où $(\alpha_{1\,j},\alpha_{2\,j},\dots,\alpha_{n\,j})$ sont les coordonnées de y_j dans la base $(x_1,x_2,\dots,x_n)$ de $\mathrm{Vect}(x_1,x_2,\dots,x_n)$. Alors, comme f est n-linéaire alternée, il existe $\alpha \in \mathbb{K}$ tel que :

$$f(y_1,\dots,y_n) = \alpha f(x_1,\dots,x_n) = \alpha$$

α dépendant uniquement des coordonnées $\alpha_{i\,j}$ des y_j. Or, comme ψ possède les mêmes propriétés que f : ψ est n-linéaire alternée, ce même α intervient dans l'égalité : $\psi(y_1,\dots,y_n) = \alpha\psi(x_1,\dots,x_n)$. D'où, si $\psi(x_1,\dots,x_n) = 1$, alors :

$$\psi(y_1,\dots,y_n) = \alpha = f(y_1,\dots,y_n).$$

Proposition 4.2.4 *Soit f une forme n-linéaire alternée sur l'espace vectoriel E. Soit $(x_1,\dots,x_n) \in E^n$. Alors, pour tout $j \in [\![1,n]\!]$, pour tout $(\lambda_1,\dots,\overset{\wedge}{\lambda_j},\dots,\lambda_n) \in \mathbb{K}^{n-1}$:*

$$f(x_1,\dots,x_j,\dots,x_n) = f\left(x_1,\dots,x_j + \sum_{\substack{i=1\\ i\neq j}}^{n} \lambda_i x_i,\dots,x_n\right).$$

Autrement dit : on ne change pas la valeur de $f(x_1,\dots,x_n)$ en ajoutant à l'un des vecteurs une combinaison linéaire des autres vecteurs du n-uplet.

Démonstration 4.2.4 En utilisant la linéarité de f par rapport à la j-ème composant du n-uplet, on obtient : $f\left(x_1,\dots,x_j + \sum_{\substack{i=1\\ i\neq j}}^{n} \lambda_i x_i,\dots,x_n\right) = f(x_1,\dots,x_j,\dots,x_n) + \sum_{\substack{i=1\\ i\neq j}}^{n} \lambda_i f(x_1,\dots,x_i,\dots,x_n)$. Or, pour tout $i \in [\![1,n]\!] \setminus \{j\}$, $f(x_1,\dots,\underbrace{x_i}_{\substack{j\text{-ème}\\ \text{composante}}},\dots,x_n) = 0$.

Théorème 4.2.5 *Soit $n \in \mathbb{N}$. Soit $(x_1,x_2,\dots,x_n)$ une famille génératrice du $\mathbb{K}$-espace vectoriel E.*
Soient $y_1,y_2,\dots,y_m$ des vecteurs de E.
Si $m > n$, alors la famille $(y_1,y_2,\dots,y_m)$ est liée.

Démonstration 4.2.5 D'après le théorème 4.2.3, si $(y_1,y_2,\dots,y_m)$ était libre, il existerait une forme m-linéaire alternée f sur $\mathrm{Vect}(y_1,y_2,\dots,y_m)$ telle que $f(y_1,y_2,\dots,y_m) = 1$. Or, nous allons montrer que toute forme m-linéaire alternée sur $\mathrm{Vect}(y_1,\dots,y_m)$ est nulle, dès lors que E possède une famille génératrice à n éléments, avec $n < m$.

Soit $f : \mathrm{Vect}(y_1,y_2,\dots,y_m)^m \to \mathbb{K}$ une application m-linéaire alternée.
Posons $F = \mathrm{Vect}(y_1,y_2,\dots,y_m)$. F est un sous-espace vectoriel de E. Partant de F, nous allons ajouter un par un

les générateurs $x_1,x_2,\ldots,x_n$, pour reconstruire E.
Si $x_1 \in F$, alors posons $F_1 = F$.
Si $x_1 \notin F$, alors posons $x_{i_1} = x_1$ et $F_1 = \mathrm{Vect}(y_1,y_2,\ldots,y_m,x_{i_1})$.
Pour $k \in [\![1, n-1]\!]$:
Si $x_{k+1} \in F_k = \mathrm{Vect}(y_1,\ldots,y_m,x_{i_1},\ldots,x_{i_p})$, alors $F_{k+1} = F_k$.
Si $x_{k+1} \notin F_k = \mathrm{Vect}(y_1,\ldots,y_m,x_{i_1},\ldots,x_{i_p})$, alors $x_{i_{p+1}} = x_{k+1}$ et $F_{k+1} = \mathrm{Vect}(y_1,y_2,\ldots,y_m,x_{i_1},\ldots,x_{i_p},x_{i_{p+1}})$.
Comme $E = \mathrm{Vect}(x_1,x_2,\ldots,x_n)$, on est certain d'avoir $F_n = E$. Il existe donc un nombre entier naturel p, inférieur ou égal à n, tel que : $E = \mathrm{Vect}(y_1,y_2,\ldots,y_m,x_{i_1},x_{i_2},\ldots,x_{i_p})$.
Montrons qu'alors pour tout x dans E, il existe un unique y élément de F et une unique combinaisons linéaire $\sum_{k\in[\![1,\,p]\!]} \lambda_k x_{i_k}$ de la famille $(x_{i_1},x_{i_2},\ldots,x_{i_p})$, tels que : $x = y + \sum_{k\in[\![1,\,p]\!]} \lambda_k x_{i_k}$.
Comme $E = \mathrm{Vect}(y_1,y_2,\ldots,y_m,x_{i_1},x_{i_2},\ldots,x_{i_p})$, alors $x = \sum_{k\in[\![1,\,m]\!]} \mu_k y_k + \sum_{k\in[\![1,\,n]\!]} \lambda_k x_{i_k}$. Or, $\sum_{k\in[\![1,\,m]\!]} \mu_k y_k \in F$. Donc, l'existence de la décomposition est avérée. Quant à l'unicité, elle découle du fait que pour tout $k \in [\![1,p]\!]$, $x_{i_k} \notin F$ et que $(x_{i_1},x_{i_2},\ldots,x_{i_p})$ est libre ou vide (preuve?).
Soit $\phi : E \to F$ l'application qui à $x = y + \sum_{k\in[\![1,\,p]\!]} \lambda_k x_{i_k}$, $y \in F$, associe y. ϕ est une application linéaire (preuve?). Si $x \in F$, alors $\phi(x) = x$. Ceci permet de définir une application m-linéaire alternée g, qui prolonge l'application f à E^m : pour tout $(a_1,a_2,\ldots,a_m) \in E^m$, $g(a_1,a_2,\ldots,a_m) = f(\phi(a_1),\phi(a_2),\ldots,\phi(a_m))$. Comme $E = \mathrm{Vect}(x_1,x_2,\ldots,x_n)$, tout $a_j \in E$ est une combinaison linéaire des x_i : $a_j = \sum_{i=1}^{n} \lambda_{i\,j} x_i$. Mais alors, en utilisant la m-linéarité de g, on obtient que $g(a_1,a_2,\ldots,a_m)$ est une somme de termes de type : un élément de $\mathbb{K}$ multiplié par $g(x_{j_1},x_{j_2},\ldots,x_{j_m})$, avec $j_k \in [\![1,n]\!]$ pour tout $f \in [\![1,m]\!]$. La famille des x_i n'ayant que n éléments et m étant strictement supérieur à n, il y a obligatoirement deux fois de même x_i parmi $(x_{j_1},x_{j_2},\ldots,x_{j_m})$; et comme g est alternée : $g(x_{j_1},x_{j_2},\ldots,x_{j_m}) = 0$. Ceci entraîne la nullité de $g(a_1,a_2,\ldots,a_m)$ pour tout $(a_1,a_2,\ldots,a_m) \in E^m$. Puisque pour tout $(a_1,a_2,\ldots,a_m) \in F^m$, $g(a_1,a_2,\ldots,a_m) = f(a_1,a_2,\ldots,a_m)$, la nullité de f est démontrée.

Corollaire 4.2.5.1 (Théorème de la dimension) *Si le $\mathbb{K}$-espace vectoriel E possède une base composée de n ($n \in \mathbb{N}$) éléments, alors toute base de E possède n éléments.*

Démonstration 4.2.5.1 Si $(x_1,x_2,\ldots,x_n)$ et $(y_i)_{i\in I}$ sont deux bases de E, alors d'après le théorème 4.2.5, I ne peut avoir strictement plus de n éléments, car sinon, la famille $(y_i)_{i\in I}$ serait liée. D'où, $(y_i)_{i\in I} = (y_1,y_2,\ldots,y_m)$ avec $m \leqslant n$. Pour les mêmes raisons, on doit avoir $n \leqslant m$. D'où, $m = n$.

Définition et notation 4.2.4 (Dimension) *Soit E un $\mathbb{K}$-espace vectoriel possédant une base à n éléments ($n \in \mathbb{N}$). Comme toute base de E a n éléments, on dit que la dimension de E sur $\mathbb{K}$ est n. Ceci s'écrit :* $\dim_{\mathbb{K}} E = n$.

Définition 4.2.5 (Espace vectoriel de dimension finie) *Si le $\mathbb{K}$-espace vectoriel E possède une base ayant un nombre fini d'éléments, on dit que E est de dimension finie.*

Corollaire 4.2.5.2 *Soit F un sous-espace vectoriel du $\mathbb{K}$-espace vectoriel de dimension finie E. Alors,* $\dim_{\mathbb{K}} F \leqslant \dim_{\mathbb{K}} E$.

Démonstration 4.2.5.2 Parmi les familles libres d'éléments de F, choisissons une famille ayant un nombre maximal d'éléments (ce nombre est $\leqslant \dim_{\mathbb{K}} E$). Alors cette famille est une base de F, car elle est libre et ne le reste pas dès qu'on lui adjoint un vecteur de F qui n'est pas dans la famille.

Corollaire 4.2.5.3 *Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}$ sur $\mathbb{K}$, et soit F un sous-espace vectoriel de E. Si* $\dim_{\mathbb{K}} F = n$, *alors $F = E$.*

Démonstration 4.2.5.3 Si la dimension commune est 0 alors $E = F = \{0_E\}$. Supposons $n > 0$. Soit $(e_1,e_2,\ldots,e_n)$ une base de F. Si $F \neq E$, alors il existe $x \in E \setminus F$. Montrons que $(e_1,e_2,\ldots,e_n,x)$ est libre. Si $\sum_{i\in[\![1,\,n]\!]} \lambda_i e_i + \lambda x = 0_E$, alors $\lambda = 0$, car sinon $x = \sum_{i\in[\![1,\,n]\!]} -\frac{\lambda_i}{\lambda} e_i \in F$. Mais, si $\lambda = 0$, comme $(e_1,\ldots,e_n)$ est libre, $\lambda_i = 0$ pour tout $i \in [\![1,n]\!]$. Or, si $\dim_{\mathbb{K}} E = n$, on ne peut avoir dans E une famille libre de $n+1$ éléments. Cette contradiction provient de l'hypothèse : $F \neq E$. Donc, $F = E$.

Corollaire 4.2.5.4 *Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}$ sur $\mathbb{K}$.*
Soit $(e_1,e_2,\ldots,e_n)$ une famille de vecteurs de E.
Alors, les trois propriétés suivantes sont équivalentes :
(i) $(e_1,e_2,\ldots,e_n)$ est une famille génératrice de E.
(ii) $(e_1,e_2,\ldots,e_n)$ est une famille libre de E.

(iii) $(e_1,e_2,\dots,e_n)$ *est une base de* E.

Démonstration 4.2.5.4 Si $(e_1,e_2,\dots,e_n)$ est libre, alors $(e_1,e_2,\dots,e_n)$ est génératrice, car sinon, il existerait $x \in E \setminus \mathrm{Vect}(e_1,e_2,\dots,e_n)$, et $(e_1,e_2,\dots,e_n,x)$ serait libre, ce qui est en contradiction avec la dimension de E.
Si $(e_1,e_2,\dots,e_n)$ est génératrice, alors $(e_1,e_2,\dots,e_n)$ est libre, car sinon, on aurait $\sum_{i\in[\![1,n]\!]} \lambda_i e_i = 0_E$ avec des λ_i non tous nuls. Supposons qu'alors, $\lambda_1 \neq 0$. Dans ce cas, $e_1 = \sum_{i=2}^{n} -\frac{\lambda_i}{\lambda_1} e_i$, et $E = \mathrm{Vect}(e_2,e_3,\dots,e_n)$. Ceci contredirait $\dim_{\mathbb{K}} E = n$, puisqu'alors n vecteurs ne pourraient constituer une famille libre.

Proposition 4.2.6 *Soit* E *un* $\mathbb{K}$*-espace vectoriel,* $E \neq \{0_E\}$*. Soit* $n \in \mathbb{N}$ *et* $(x_1,x_2,\dots,x_n)$ *une famille génératrice* E*. Il existe* $I \subset [\![1,n]\!]$ *tel que* $(x_i)_{i\in I}$ *soit une base de* E.

Démonstration 4.2.6 Démontrons la proposition par récurrence sur n. Si $n = 1$, alors (x_1) est une base, car $x_1 \neq 0_E$. Supposons que la proposition soit vrai pour un nombre entier n. Montrons qu'alors elle est vraie pour $n+1$. Soit $(x_1,x_2,\dots,x_{n+1})$ une famille génératrice de E. Si $x_{n+1} \in \mathrm{Vect}(x_1,x_2,\dots,x_n)$, alors $E = \mathrm{Vect}(x_1,x_2,\dots,x_n)$ et il suffit d'appliquer l'hypothèse de récurrence à $(x_1,x_2,\dots,x_n)$. Si $x_{n+1} \notin \mathrm{Vect}(x_1,x_2,\dots,x_n)$, considérons la base $(x_{i_1},x_{i_2},\dots,x_{i_p})$ de $\mathrm{Vect}(x_1,x_2,\dots,x_n)$, formée de vecteurs de la famille $(x_1,\dots,x_n)$. On a alors : $E = \mathrm{Vect}(x_{i_1},\dots,x_{i_p},x_{n+1})$. Il ne reste plus qu'à montrer que la famille $(x_{i_1},\dots,x_{i_p},x_{n+1})$ est libre. Supposons la combinaison linéaire : $\sum_{k=1}^{p} \lambda_k x_{i_k} + \lambda x_{n+1}$ égale au vecteur nul. Alors, $\lambda = 0$, car sinon, on aurait $x_{n+1} \in \mathrm{Vect}(x_{i_1},\dots,x_{i_p})$. Mais alors, comme $(x_{i_1},\dots,x_{i_p})$ est libre, on a : $\lambda_k = 0$ pour tout $k \in [\![1,p]\!]$.

La proposition 4.2.6 nous indique que tout espace vectoriel,non réduit à son vecteur nul, ayant une famille génératrice finie est de dimension finie. Rappelons que l'espace vectoriel réduit à son vecteur nul est de dimension 0 et admet la famille vide (ayant 0 éléments) comme famille génératrice. Il est fréquent de donner comme définition d'un espace vectoriel de dimension fini : espace vectoriel ayant une famile génératrice finie. Le cas particulier de l'espace vectoriel réduit à son vecteur nul

Corollaire 4.2.6.1 (Théorème de la base incomplète) *Soit* $n \in \mathbb{N}$*. Considérons le* $\mathbb{K}$*-espace vectoriel* E *de dimension* n*. Soit* $(x_1,x_2,\dots,x_p)$ *une famille libre de vecteurs de* E *(*$p \leqslant n$*, d'après le théorème 4.2.5). Il existe alors* $n-p$ *vecteurs :* $y_1,y_2,\dots,y_{n-p}$*, tels que :* $(x_1,\dots,x_p,y_1,\dots,y_{n-p})$ *soit une base de* E.

Démonstration 4.2.6.1 Il suffit de considérer la famille génératrice : $(x_1,\dots,x_p,e_1,\dots,e_n)$, où $(e_1,\dots,e_n)$ est une base de E, et de reprendre la démonstration de la proposition 4.2.6 avec $(x_1,x_2,\dots,x_p)$ comme famille de départ, à laquelle on ajoute certains des e_i, de sorte à obtenir une famille libre et génératrice de E.

4.3 Déterminants

Définition et notation 4.3.1 (Déterminant) *Soit* E *un* $\mathbb{K}$*-espace vectoriel de dimension finie* n*,* $n \geqslant 1$ *(*$E \neq \{0_E\}$*). Soit* $e = (e_1,e_2,\dots,e_n)$ *une base de* E.
Le déterminant dans la base e *est l'unique* [9] *forme* n*-linéaire alternée définie sur* E^n*, notée* $\det_e$*, telle que :* $\det_e(e_1,e_2,\dots,e_n) = 1$.

Théorème 4.3.1 *Soit* $e = (e_1,e_2,\dots,e_n)$*,* $n \geqslant 1$*, une base du* $\mathbb{K}$*-espace vectoriel* E.
La famille $(x_1,x_2,\dots,x_n)$ *est libre, si et seulement si*

$$\det_e(x_1,x_2,\dots,x_n) \neq 0.$$

Démonstration 4.3.1 D'après la proposition 4.2.2 de la page 41, si $\det_e(x_1,x_2,\dots,x_n) \neq 0$, alors $(x_1,x_2,\dots,x_n)$ est libre.

Réciproquement : supposons $(x_1,x_2,\dots,x_n)$ libre. D'après le corollaire 4.2.5.4 page 43, $(x_1,x_2,\dots,x_n)$ est une base de E. D'après le théorème 4.2.3 page 41, il existe une unique forme n-linéaire alternée f, définie sur $(\mathrm{Vect}(x_1,x_2,\dots,x_n))^n = E^n$, telle que : $f(x_1,x_2,\dots,x_n) = 1$. D'après le définition 4.3.1, cette forme f est le déterminant dans la base $x = (x_1,x_2,\dots,x_n)$. En utilisant les propriétés de $\det_x$, forme n-linéaire alternée, ainsi que le fait que chaque x_i est une combinaison linéaire des e_j, on obtient l'existence de α dans $\mathbb{K}$, dépendant uniquement des coordonnées des x_i dans la base e, et tel que : $\det_x(x_1,x_2,\dots,x_n) = \alpha \det_x(e_1,e_2,\dots,e_n)$. Comme $\det_x(x_1,x_2,\dots,x_n) = 1$, on a : $\alpha \in \mathbb{K}^*$. Comme $\det_e$ est une forme n-linéaire alternée, au même titre que $\det_x$, on a : $\alpha = \alpha \det_e(e_1,e_2,\dots,e_n) = \det_e(x_1,x_2,\dots,x_n)$. D'où, $\det_e(x_1,x_2,\dots,x_n) \neq 0$.

9. cf : théorème 4.2.3.

Théorème 4.3.2 *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \geqslant 1$.*
Soit $e = (e_1,e_2,\dots,e_n)$ une base de E.
Soit $f : E^n \to \mathbb{K}$ une forme n-linéaire alternée.
Il existe alors un unique $\alpha \in \mathbb{K}$ tel que : $f = \alpha \det_e$.

Démonstration 4.3.2 Comme f et $\det_e$ sont n-linéaires alternées, pour tout $(x_1,x_2,\dots,x_n) \in E^n$, il existe un unique $\lambda \in \mathbb{K}$ tel que : $f(x_1,x_2,\dots,x_n) = \lambda f(e_1,e_2,\dots,e_n)$ et $\det_e(x_1,x_2,\dots,x_n) = \lambda \det_e(e_1,e_2,\dots,e_n) = \lambda$. Ce scalaire λ ne dépend que des coordonnées des x_i dans la base e. On déduit des égalités précédentes :

$$f(x_1,x_2,\dots,x_n) = \det_e(x_1,x_2,\dots,x_n) f(e_1,e_2,\dots,e_n).$$

D'où, le scalaire α de l'énoncé existe et est uniquement déterminé, puisque $\alpha = f(e_1,e_2,\dots,e_n)$.

4.3.1 Calculs de déterminants

Fixons un $\mathbb{K}$-espace vectoriel E, de dimension finie $n \geqslant 1$, et $e = (e_1,e_2,\dots,e_n)$ une base de E.

Définition et notation 4.3.2 (Matrice d'un système de vecteurs) *Soit $(x_1,x_2,\dots,x_n)$ un système de vecteurs de E. Pour tout $j \in [\![1,n]\!]$, notons $(x_{1\,j},x_{2\,j},\dots,x_{n\,j})$ les coordonnées de x_j dans la base e.*

Le tableau de scalaires : $M = \begin{pmatrix} x_{1\,1} & x_{1\,2} & \cdots & x_{1\,n} \\ x_{2\,1} & x_{2\,2} & \cdots & x_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n\,1} & x_{n\,2} & \cdots & x_{n\,n} \end{pmatrix} = \left(x_{i\,j}\right)_{(i,j)\in[\![1,\,n]\!]\times[\![1,\,n]\!]}$

s'appelle la matrice du système $(x_1,x_2,\dots,x_n)$ dans la base e. Comme la matrice M est composée de n lignes et de n colonnes, on dit que M est une matrice carrée $n \times n$. $x_{i\,j}$ se trouve dans la i-ème ligne et la j-ème colonne de M.

Remarque : dans la colonne j de la matrice M de la définition 4.3.2, on lit les coordonnées de x_j dans le base e. Si la matrice M a autant de lignes que de colonnes, c'est parce que $\dim_{\mathbb{K}} E = n$ et que le système des x_i comporte n vecteurs. Des matrices de tailles différentes existent, mais nous n'avons pas, pour l'instant, a nous en préoccuper.

Notation 4.3.3 *L'ensemble des matrices n lignes, n colonnes, $n \geqslant 1$, à coefficients dans $\mathbb{K}$ se note : $\mathcal{M}_n(\mathbb{K})$.*

Définition et notation 4.3.4 (Déterminant d'une matrice $n \times n$) *Soit $(x_1,x_2,\dots,x_n)$, $n \geqslant 1$, un système de vecteurs de E. Pour tout j dans $[\![1,n]\!]$, les coordonnées de x_j dans la base e sont : $(x_{1\,j},x_{2\,j},\dots,x_{n\,j})$.*

Le déterminant de la matrice $M = \begin{pmatrix} x_{1\,1} & x_{1\,2} & \cdots & x_{1\,n} \\ x_{2\,1} & x_{2\,2} & \cdots & x_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n\,1} & x_{n\,2} & \cdots & x_{n\,n} \end{pmatrix}$ est le déterminant dans la base e du système $(x_1,x_2,\dots,x_n)$.

Ce déterminant est noté : $\det M$ *ou* $\begin{vmatrix} x_{1\,1} & x_{1\,2} & \cdots & x_{1\,n} \\ x_{2\,1} & x_{2\,2} & \cdots & x_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n\,1} & x_{n\,2} & \cdots & x_{n\,n} \end{vmatrix}$.

Exercice 4.3.1 *On considère le $\mathbb{R}$-espace vectoriel $\mathbb{R}^2$ muni de la base canonique $e = ((1,0),(0,1))$.*

1. *Montrer que $\psi : (\mathbb{R}^2)^2 \to \mathbb{R}$, définie par $\psi((a,b),(c,d)) = ad - bc$, est bilinéaire (2-linéaire) alternée.*
2. *Soient $\alpha = (a,b)$ et $\beta = (c,d)$ des vecteurs de $\mathbb{R}^2$.*
   Que vaut $\det_e(\alpha,\beta)$?
3. *Calculer* $\begin{vmatrix} -1 & 1 \\ 1 & 2 \end{vmatrix}$.

Notation 4.3.5 *On note I_n l'élément de $\mathcal{M}_n(\mathbb{K})$ définie par :*

$$I_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix} = \left(\delta_{i\,j}\right)_{(i,j)\in[\![1,\,n]\!]\times[\![1,\,n]\!]}$$

I_n est la matrice du système $(e_1,e_2,\dots,e_n)$ dans la base $(e_1,e_2,\dots,e_n)$. D'où, $\det I_n = 1$.

Définition et notation 4.3.6 (Cofacteur) *Soit $M \in \mathcal{M}_n(\mathbb{K})$, $n \geqslant 2$.*

$$M = \Big(x_{i\,j}\Big)_{(i,j)\in[\![1,\,n]\!]\times[\![1,\,n]\!]}$$

Soit $M_{i\,j} \in \mathcal{M}_{n-1}(\mathbb{K})$, la matrice obtenue à partir de M, en supprimant la ligne i et la colonne j de M :

$$M_{ij} = \left(\begin{array}{ccccc} x_{1\,1} & \cdots & \multicolumn{1}{c|}{x_{1\,j}} & \cdots & x_{1\,n} \\ \vdots & & & & \vdots \\ \cline{3-3} x_{i\,1} & & \multicolumn{1}{c|}{x_{i\,j}} & & x_{j\,n} \\ \cline{3-3} \vdots & & & & \vdots \\ x_{n\,1} & \cdots & x_{n\,j} & \cdots & x_{n\,n} \end{array}\right) \begin{array}{l} \\ \\ \\ \leftarrow \textit{ligne } i \\ \\ \\ \end{array}$$

$$\textit{colonne } j \downarrow$$

On appelle cofacteur de $x_{i\,j}$, l'élément de $\mathbb{K}$ noté $A_{i\,j}$ et définit par :

$$A_{i\,j} = (-1)^{i+j} \det M_{i\,j}.$$

La matrice M ayant n lignes et n colonnes, on remarque que $M_{i\,j}$ est bien une matrice $n-1$ lignes, $n-1$ colonnes :

Développement par rapport à la première ligne

Un principe général de calcul de déterminants est de réduire en quelques étapes, la taille des matrices, pour se ramener à des calculs de déterminants sur des matrices 2×2 (voir l'exercice 4.3.1). La démonstration du théorème 4.2.3 page 41 nous fournit un mode d'emploi pour passer du déterminant d'une matrice $n \times n$ à des déterminants de matrices $(n-1) \times (n-1)$. En effet, toutes matrice $n \times n$ peut être interprétée comme une matrice des coordonnées de n vecteurs de $\mathbb{K}^n$ dans une base quelconque de $\mathbb{K}^n$.

Soit $M = \begin{pmatrix} x_{1\,1} & x_{1\,2} & \cdots & x_{1\,n} \\ x_{2\,1} & x_{2\,2} & \cdots & x_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n\,1} & x_{n\,2} & \cdots & x_{n\,n} \end{pmatrix} \in \mathcal{M}_n(\mathbb{K})$.

Pour $j \in [\![1,n]\!]$, posons : $x_j = (x_{1\,j},x_{2\,j},\dots,x_{n\,j}) \in \mathbb{K}^n$.

Nous avons donc : $\det M = \det_e(x_1,x_2,\dots,x_n)$, où e désigne la base canonique de $\mathbb{K}^n$; autrement dit : $e = (e_1,e_2,\dots,e_n)$ avec pour tout j dans $[\![1,n]\!]$, $e_j = (0,\dots,0,\underbrace{1}_{\substack{j-ème \\ place}},0,\dots,0)$.

D'après la définition de f à l'aide de g dans la démonstration du théorème 4.2.3, puisque f est l'unique forme n-linéaire alternée telle que : $f(e_1,e_2,\dots,e_n) = 1$ (la base ici utilisée n'est plus $(x_1,x_2,\dots,x_n)$, mais $(e_1,e_2,\dots,e_n)$), et puisque g est l'unique forme $n-1$-linéaire alternée telle que : $g(e_2,e_3,\dots,e_n) = 1$, on a :

$$f = \det_e$$

$$g = \det_{e'}$$

$$\det M = \det_e(x_1,x_2,\dots,x_n) = \sum_{j\in[\![1,\,n]\!]} (-1)^{j+1} x_{1\,j} \det_{e'}(a_1,\dots,\overset{\wedge}{a_j},\dots,a_n)$$

avec $e' = (e_2,e_3,\dots,e_n)$ base de $\mathrm{Vect}(e_2,e_3,\dots,e_n)$, et pour $j \in [\![1,n]\!]$, $x_j = x_{1\,j}e_1 + a_j$, $a_j = \sum_{i=2}^n x_{i\,j}e_i \in \mathrm{Vect}(e_2,e_3,\dots,e_n)$.

On en déduit :

$$\begin{vmatrix} x_{1\,1} & x_{1\,2} & \cdots & x_{1\,n} \\ x_{2\,1} & x_{2\,2} & \cdots & x_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n\,1} & x_{n\,2} & \cdots & x_{n\,n} \end{vmatrix} = \sum_{j=1}^{n} (-1)^{j+1} x_{1\,j} \begin{vmatrix} x_{2\,1} & \cdots & x_{2\,j-1} & x_{2\,j+1} & \cdots & x_{2\,n} \\ x_{3\,1} & \cdots & x_{3\,j-1} & x_{3\,j+1} & \cdots & x_{3\,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_{n\,1} & \cdots & x_{n\,j-1} & x_{n\,j+1} & \cdots & x_{n\,n} \end{vmatrix}$$

$$= \sum_{j=1}^{n} x_{1\,j} A_{1\,j}$$

$A_{1\,j}$ étant le cofacteur de $x_{1\,j}$ dans la matrice M.

Développement par rapport à la i-ème ligne

Notons e^i la base obtenue à partir de e en ramenant le i-ème vecteur de la base à la première place :

$$e^i = (e_i,e_1,\ldots,e_{i-1},e_{i+1},\ldots,e_n)$$

Soit $M \in \mathcal{M}_n(\mathbb{K})$, $M = \left(x_{i\,j}\right)_{(i,j)\in[\![1,\,n]\!]^2}$.
Considérons M comme la matrice du système $(x_1,x_2,\ldots,x_n)$ dans la base e. Nous avons obtenu lors de la démonstration du théorème 4.3.2 page 45, que si f est une forme n-linéaire alternée sur E ($\dim_{\mathbb{K}} E = n$), alors :

$$f(x_1,x_2,\ldots,x_n) = f(e_1,e_2,\ldots,e_n)\det{}_e(x_1,x_2,\ldots,x_n)$$

On en déduit, en prenant pour f : $\det_e$, et pour $\det_e$: $\det_{e^i}$:

$$\det{}_e(x_1,x_2,\ldots,x_n) = \det{}_e(e_i,e_1,\ldots,e_{i-1},e_{i+1},\ldots,e_n)\det{}_{e^i}(x_1,x_2,\ldots,x_n)$$

Or, $1 = \det_e(e_1,e_2,\ldots,e_n) = (-1)^{i+1}\det_e(e_i,e_1,\ldots,e_{i-1},e_{i+1},\ldots,e_n)$.
Qu'est-ce que $\det_{e^i}(x_1,x_2,\ldots,x_n)$?

$$\det{}_{e^i}(x_1,x_2,\ldots,x_n) = \begin{vmatrix} x_{i\,1} & x_{i\,2} & \cdots & x_{i\,n} \\ x_{1\,1} & x_{1\,2} & \cdots & x_{1\,n} \\ \vdots & \vdots & & \vdots \\ x_{i-1\,1} & x_{i-1\,2} & \cdots & x_{i-1\,n} \\ x_{i+1\,1} & x_{i+1\,2} & \cdots & x_{i+1\,n} \\ \vdots & \vdots & & \vdots \\ x_{n\,1} & x_{n\,2} & \cdots & x_{n\,n} \end{vmatrix}$$

Développons ce déterminant par rapport à la première ligne. Nous avons :

$$\det{}_{e^i}(x_1,x_2,\ldots,x_n) = \sum_{j=1}^{n}(-1)^{j+1}x_{i\,j}\det M_{i\,j}$$

où $M_{i\,j}$ est la matrice utilisée dans la définition du cofacteur de $x_{i\,j}$ dans la matrice M (voir page 46). On obtient le développement du déterminant de M par rapport à sa i-ème ligne :

$$\begin{aligned} \det M &= \det{}_e(x_1,x_2,\ldots,x_n) \\ &= (-1)^{i+1}\det{}_{e^i}(x_1,x_2,\ldots,x_n) \\ &= (-1)^{i+1}\sum_{j=1}^{n}(-1)^{j+1}x_{i\,j}\det M_{i\,j} \\ &= \sum_{j=1}^{n}x_{i\,j}A_{i\,j} \end{aligned}$$

Déterminant de la transposée

Définition et notation 4.3.7 (Matrice transposée) *Soit $M \in \mathcal{M}_n(\mathbb{K})$. La transposée de M est l'élément de $\mathcal{M}_n(\mathbb{K})$ noté ${}^tM$, et défini de la façon suivante : pour tout $j \in [\![1,n]\!]$, la ligne j de ${}^tM$ est la colonne j de M. Autrement dit : si $M = \left(x_{i\,j}\right)$ alors ${}^tM = \left(x_{j\,i}\right)$.*

Théorème 4.3.3 $\det {}^tM = \det M$

Démonstration 4.3.3 Montrons le théorème par récurrence sur l'entier n, pour tout M dans $\mathcal{M}_n(\mathbb{K})$.
Si $M \in \mathcal{M}_1(\mathbb{K})$, alors $M = (x_{1\,1}) = {}^tM$ et $\det M = \det {}^tM = x_{1\,1}$.
Soit $n \in \mathbb{N}$, $n > 1$. Supposons que pour tout $m \in [\![1,n-1]\!]$, et toute matrice $N \in \mathcal{M}_m(\mathbb{K})$, on ait : $\det {}^tN = \det N$.
Soit $M \in \mathcal{M}_n(\mathbb{K})$. $M = \left(x_{i\,j}\right)_{(i,j)\in[\![1,\,n]\!]^2}$.
Notons $(y_1,y_2,\ldots,y_n)$ le système de vecteurs de E dont la matrice dans la base $e = (e_1,e_2,\ldots,e_n)$ de E est ${}^tM$.

Alors, $\det {}^tM = \det_e(y_1,y_2,\ldots,y_n)$. D'autre part, pour tout $j \in [\![1,n]\!]$, $y_j = \sum_{i=1}^n x_{j\,i} e_i$, puisque la j-ème colonne de ${}^tM$ est égale à la j-ème ligne de M. On en déduit :

$$\begin{aligned}
\det {}^tM &= \det_e(y_1,y_2,\ldots,y_n) \\
&= \det_e\left(\sum_{i=1}^n x_{1\,i} e_i, y_2, \ldots, y_n\right) \\
&= \sum_{i=1}^n x_{1\,i} \det_e(e_i,y_2,\ldots,y_n) \\
&= \sum_{i=1}^n x_{1\,i} (-1)^{i+1} \det_{e^i}(e_i,y_2,\ldots,y_n)
\end{aligned}$$

avec $e^i = (e_i,e_1,\ldots,e_{i-1},e_{i+1},\ldots,e_n)$.
Comme $\det_{e^i}$ est alternée, on a :

$$\begin{aligned}
\det_{e^i}(e_i,y_2,\ldots,y_n) &= \det_{e^i}\left(e_i, \sum_{k=1}^n x_{2\,k} e_k, \ldots, \sum_{k=1}^n x_{n\,k} e_k\right) \\
&= \det_{e^i}\left(e_i, \sum_{\substack{k=1 \\ k\neq i}}^n x_{2\,k} e_k, \ldots, \sum_{\substack{k=1 \\ k\neq i}}^n x_{n\,k} e_k\right) \\
&= \begin{vmatrix}
1 & 0 & \cdots & 0 \\
0 & x_{2\,1} & \cdots & x_{n\,1} \\
\vdots & \vdots & & \vdots \\
0 & x_{2\,i-1} & \cdots & x_{n\,i-1} \\
0 & x_{2\,i+1} & \cdots & x_{n\,i+1} \\
\vdots & \vdots & & \vdots \\
0 & x_{2\,n} & \cdots & x_{n\,n}
\end{vmatrix}
\end{aligned}$$

Alors, en développant ce déterminant par rapport à la première ligne, on obtient :

$$\begin{vmatrix}
1 & 0 & \cdots & 0 \\
0 & x_{2\,1} & \cdots & x_{n\,1} \\
\vdots & \vdots & & \vdots \\
0 & x_{2\,i-1} & \cdots & x_{n\,i-1} \\
0 & x_{2\,i+1} & \cdots & x_{n\,i+1} \\
\vdots & \vdots & & \vdots \\
0 & x_{2\,n} & \cdots & x_{n\,n}
\end{vmatrix} = \begin{vmatrix}
x_{2\,1} & \cdots & x_{n\,1} \\
\vdots & & \vdots \\
x_{2\,i-1} & \cdots & x_{n\,i-1} \\
x_{2\,i+1} & \cdots & x_{n\,i+1} \\
\vdots & & \vdots \\
x_{2\,n} & \cdots & x_{n\,n}
\end{vmatrix}$$

En utilisant l'hypothèse de récurrence sur ce déterminant $(n-1)\times(n-1)$:

$$\begin{vmatrix}
x_{2\,1} & \cdots & x_{n\,1} \\
\vdots & & \vdots \\
x_{2\,i-1} & \cdots & x_{n\,i-1} \\
x_{2\,i+1} & \cdots & x_{n\,i+1} \\
\vdots & & \vdots \\
x_{2\,n} & \cdots & x_{n\,n}
\end{vmatrix} = \det M_{1\,i}$$

où $M_{1\,i}$ est la matrice $(n-1)\times(n-1)$ déduite de M, en supprimant sa i-ème ligne et sa j-ème colonne.
Nous avons obtenu :

$$\begin{aligned}
\det {}^tM &= \sum_{i=1}^n x_{1\,j} (-1)^{i+1} \det M_{1\,j} \\
&= \sum_{i=1}^n x_{1\,j} A_{1\,j}
\end{aligned}$$

Or, nous reconnaissons dans le dernier membre le développement du déterminant de M par rapport à sa première ligne. D'où le théorème.

Développement par rapport à la j-ème colonne

Nous avons déjà obtenu le développement du déterminant d'une matrice $M \in \mathcal{M}_n(\mathbb{K})$ par rapport à sa i-ème ligne. D'après le théorème 4.3.3, pour obtenir le développement de $\det M$ par rapport à la j-ème colonne, il suffit d'écrire le développement de $\det {}^tM$ par rapport à sa j-ème ligne.

D'où, si $M = \begin{pmatrix} x_{1\,1} & \cdots & x_{1\,n} \\ \vdots & \ddots & \vdots \\ x_{n\,1} & \cdots & x_{n\,n} \end{pmatrix}$, alors :

$$\det M = \sum_{i=1}^{n} x_{i\,j} A_{i\,j}$$

$A_{i\,j}$ étant le cofacteur de $x_{i\,j}$.

Développement par blocs

Proposition 4.3.4 *Soit $M \in \mathcal{M}_n(\mathbb{K})$, $n \geqslant 2$. Supposons qu'il existe des matrices carrées R et S, un bloc de scalaires [10] : T, et un bloc [11] de 0 : $\underline{0}$, tels que :*

$$M = \left(\begin{array}{c|c} R & T \\ \hline \underline{0} & S \end{array}\right).$$

Alors,

$$\det M = \det R \det S.$$

Démonstration 4.3.4 Montrons la proposition, par récurrence sur l'entier n. Pour $n = 2$, on a : $M = \begin{pmatrix} r & t \\ 0 & s \end{pmatrix}$, et donc $\det M = rs - 0t = ab = \det(r)\det(s)$; la propriété est vérifiée. Supposons la proposition démontrée pour tout nombre entier k, $2 \leqslant k < n$. Supposons que R soit une matrice carrée $m \times m$. Développons le déterminant de $M = \left(x_{i\,j}\right)_{(i,\,j)\in[\![1,\,n]\!]\times[\![1,\,n]\!]}$ par rapport à sa première colonne. En reprenant les notations de la définition 4.3.6, page 46, On a : $\det M = \sum_{i=1}^{n}(-1)^{i+1}x_{i\,1}\det M_{i\,1} = \sum_{i=1}^{m}(-1)^{i+1}x_{i\,1}\det M_{i\,1}$, car $x_{i\,1} = 0$ si $i > m$. On peut alors appliquer l'hypothèse de récurrence à chacune des matrices $M_{i\,1}$. On a : $\det M_{i\,1} = \det R_{i\,1}\det S$, $R_{i\,1}$ étant la matrice obtenue à partir de R en supprimant sa i-ème ligne et sa première colonne. Mais alors : $\det M = \sum_{i=1}^{m}(-1)^{i+1}x_{i\,1}\det R_{i\,1}\det S = \left(\sum_{i=1}^{m}(-1)^{i+1}x_{i\,1}\det R_{i\,1}\right)\det S = \det R \det S$.

Proposition 4.3.5 *Soit $M \in \mathcal{M}_n(\mathbb{K})$, $n \geqslant 2$. Supposons qu'il existe des matrices carrées R et S, un bloc de scalaires : T, et un bloc de 0 : $\underline{0}$, tels que :*

$$M = \left(\begin{array}{c|c} R & \underline{0} \\ \hline T & S \end{array}\right).$$

Alors,

$$\det M = \det R \det S.$$

Démonstration 4.3.5 Il suffit de reprendre les étapes de la démonstration de la proposition 4.3.4, en developpant le déterminant de M par rapport à sa première ligne.

Définition 4.3.8 (Matrice triangulaire supérieure) *Soit $M = \begin{pmatrix} x_{1\,1} & x_{1\,2} & \cdots & x_{1,\,n} \\ x_{2\,1} & x_{2\,2} & \cdots & x_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n\,1} & x_{n\,2} & \cdots & x_{n\,n} \end{pmatrix}$ un élément de $\mathcal{M}_n(\mathbb{K})$. On dit que M est une matrice triangulaire supérieure lorsque $x_{i\,j} = 0$ pour $i > j$.*

Définition 4.3.9 (Matrice triangulaire inférieure) *Soit $M = \begin{pmatrix} x_{1\,1} & x_{1\,2} & \cdots & x_{1,\,n} \\ x_{2\,1} & x_{2\,2} & \cdots & x_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n\,1} & x_{n\,2} & \cdots & x_{n\,n} \end{pmatrix}$ un élément de $\mathcal{M}_n(\mathbb{K})$. On dit que M est une matrice triangulaire inférieure lorsque $x_{i\,j} = 0$ pour $i < j$.*

10. T est une matrice (voir la définition 4.3.14, page 51).
11. $\underline{0}$ est une matrice (voir la définition 4.3.14) nulle.

Définition 4.3.10 (Diagonale) *Soit* $M = \begin{pmatrix} x_{1\,1} & \cdots & x_{1\,n} \\ \vdots & \ddots & \vdots \\ x_{n\,1} & \cdots & x_{n\,n} \end{pmatrix}$ *un élément de* $\mathcal{M}_n(\mathbb{K})$. *La diagonale de* M *est le* n*-uplet* $(x_{1\,1},x_{2\,2},\ldots,x_{n\,n})$. *Les coefficients* $x_{i\,i}$, i *dans* $[\![1,n]\!]$, *sont les coefficients diagonaux de* M.

Définition 4.3.11 (Matrice diagonale) *Soit* M *un élément de* $\mathcal{M}_n(\mathbb{K})$. *On dit que* M *est une matrice diagonale si* M *est à la fois une matrice triangulaire supérieure et une matrice triangulaire inférieure. Lorsque* M *est diagonale, tous ses coefficients, sauf éventuellement ceux de sa diagonale, sont nuls.*

Corollaire 4.3.5.1 *Soit* $M \in \mathcal{M}_n(\mathbb{K})$.

$$M = \begin{pmatrix} x_{1\,1} & x_{1\,2} & \cdots & x_{1,\,n} \\ x_{2\,1} & x_{2\,2} & \cdots & x_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n\,1} & x_{n\,2} & \cdots & x_{n\,n} \end{pmatrix}$$

Si M *est triangulaire supérieure ou triangulaire inférieure, alors*

$$\det M = x_{1\,1}x_{2\,2}\cdots x_{n-1\,n-1}x_{n\,n},$$

le déterminant est le produit des termes diagonaux.

Le corollaire 4.3.5.1 s'applique bien sur dans le cas où M est diagonale. On retrouve, par le corollaire 4.3.5.1, le résultat fondamental : $\det I_n = 1$.

Démonstration 4.3.5.1 Il suffit d'appliquer n fois de suite la proposition 4.3.4 ou la proposition 4.3.5.

4.3.2 Systèmes de Cramer

Définition 4.3.12 (Système de Cramer) *Soit* n *un nombre entier naturel différent de zéro. Soient* $a_{i\,j} \in \mathbb{K}$ *pour* $i \in [\![1,n]\!]$ *et* $j \in [\![1,n]\!]$. *Soit* $(b_1,b_2,\ldots,b_n) \in \mathbb{K}^n$. *Considérons le système* (S) *de* n *équations linéaires à* n *inconnues* $x_1,\ldots,x_n$ *:*

$$(S) \quad \left\{ \begin{array}{ccccccccccc} a_{1\,1}x_1 & + & a_{1\,2}x_2 & + & \cdots & + & a_{1\,n}x_n & = & b_1 \\ a_{2\,1}x_1 & + & a_{2\,2}x_2 & + & \cdots & + & a_{2\,n}x_n & = & b_2 \\ \vdots & & \vdots & & \vdots & & \vdots & \vdots & \vdots \\ a_{n\,1}x_1 & + & a_{n\,2}x_2 & + & \cdots & + & a_{n\,n}x_n & = & b_n \end{array} \right.$$

Ce système est dit de Cramer, si :

$$\det M = \begin{vmatrix} a_{1\,1} & a_{1\,2} & \cdots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \cdots & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n\,1} & a_{n\,2} & \cdots & a_{n\,n} \end{vmatrix} \neq 0.$$

Théorème 4.3.6 *On considère le système de Cramer :*

$$(S) \quad \left\{ \begin{array}{ccccccccccc} a_{1\,1}x_1 & + & a_{1\,2}x_2 & + & \cdots & + & a_{1\,n}x_n & = & b_1 \\ a_{2\,1}x_1 & + & a_{2\,2}x_2 & + & \cdots & + & a_{2\,n}x_n & = & b_2 \\ \vdots & & \vdots & & \vdots & & \vdots & \vdots & \vdots \\ a_{n\,1}x_1 & + & a_{n\,2}x_2 & + & \cdots & + & a_{n\,n}x_n & = & b_n \end{array} \right.$$

Avec les notations utilisées dans la définition 4.3.12, si M_k *désigne la matrice obtenue en remplaçant dans* M *la* k*-ème colonne par :* $\begin{matrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{matrix}$ *, alors :* $x_k = \dfrac{\det M_k}{\det M}$.

Démonstration 4.3.6 Plaçons nous dans l'espace vectoriel $\mathbb{K}^n$ muni de la base $e = (e_1,e_2,\ldots,e_n)$. Notons b l'élément de $\mathbb{K}^n$ dont les coordonnées dans la base e sont : $(b_1,b_2,\ldots,b_n)$. Notons, pour $j \in [\![1,n]\!]$, a_j le vecteur de $\mathbb{K}^n$ dont les coordonnées dans la base e sont : $(a_{1\,j},a_{2\,j},\ldots,a_{n\,j})$. Puisque $\det M = \det_e(a_1,a_2,\ldots,a_n) \neq 0$, les n vecteurs dont les coordonnées sont les colonnes de M : les vecteurs a_j, $j \in [\![1,n]\!]$, sont linéairement indépendants et forment donc une base de E. Puisqu'il en est ainsi, il existe un unique n-uplet $(\lambda_1,\lambda_2,\ldots,\lambda_n)$ dans $\mathbb{K}^n$ tel que :

$$b = \sum_{j\in[\![1,\,n]\!]} \lambda_j a_j$$

Mais alors, la solution du système est : $(\lambda_1,\lambda_2,\ldots,\lambda_n)$.
Remplaçons dans M la colonne k par les coordonnées de b. On obtient M_k, dont le déterminant vaut :

$$\begin{aligned}
&\det_e(a_1,\ldots,a_{k-1},b,a_{k+1},\ldots,a_n)\\
&= \det_e\left(a_1,\ldots,a_{k-1},\sum_{j\in[\![1,\,n]\!]}\lambda_j a_j,a_{k+1},\ldots,a_n\right)\\
&= \sum_{j\in[\![1,\,n]\!]}\lambda_j \det_e(a_1,\ldots,a_{k-1},a_j,\ldots,a_n)\\
&= \lambda_k \det_e(a_1,\ldots,a_{k-1},a_k,a_{k+1},\ldots,a_n)\\
&= \lambda_k \det M
\end{aligned}$$

D'où le théorème.

Bien que les systèmes de Cramer soient ici présentés en toute généralité, il est bien difficile de faire fonctionner cette belle théorie dès que le système comporte plus de trois inconnues, car les calculs de déterminants deviennent trop compliqués et trop longs.

4.3.3 Rang

Définition 4.3.13 (Rang) *Considérons un $\mathbb{K}$-espace vectoriel E. Soit I un ensemble fini. Soit $(x_i)_{i\in I}$ une famille de vecteurs de E. Le rang de la famille $(x_i)_{i\in I}$ est la dimension du sous-espace vectoriel de E engendré par cette famille.*

Nous disposons d'une première version de la notion de matrice (voir page 45) dans le cadre des coordonnées d'une famille de vecteurs. Le définition ci-dessous est plus générale.

Définition et notation 4.3.14 (Matrice à coefficients dans $\mathbb{K}$) *Soient I et J des ensembles finis et non vides. Une matrice M de type $I \times J$, à coefficients dans $\mathbb{K}$, est une application de $I \times J$ dans $\mathbb{K}$.*

$$M : I \times J \to \mathbb{K},\ (i,j) \mapsto a_{i\,j}$$

La notation usuelle de la matrice M ainsi définie est :

$$M = \left(a_{i\,j}\right)_{(i,\,j)\in I\times J}$$

Si $I = [\![1,m]\!]$ et $J = [\![1,n]\!]$, m et n étant des nombres entiers strictement positifs, alors

$$M = \begin{pmatrix} a_{1\,1} & a_{1\,2} & \cdots & a_{1\,n}\\ a_{2\,1} & a_{2\,2} & \cdots & a_{2\,n}\\ \vdots & \vdots & & \vdots\\ a_{m\,1} & a_{m\,2} & \cdots & a_{m\,n}\end{pmatrix}$$

est dans ce cas une matrice à m lignes et n colonnes.

Définition 4.3.15 (Vecteur ligne) *Soit $M : [\![1,m]\!] \times [\![1,n]\!] \to \mathbb{K}$, $(i,j) \mapsto a_{i\,j}$, une matrice ($mn > 0$). Les m vecteurs lignes de M sont les éléments $(a_{i\,1},a_{i\,2},\ldots,a_{i\,n})$ de $\mathbb{K}^n$, $i \in [\![1,m]\!]$.*

Définition 4.3.16 (Vecteur colonne) *Soit $M : [\![1,m]\!] \times [\![1,n]\!] \to \mathbb{K}$, $(i,j) \mapsto a_{i\,j}$, une matrice ($mn > 0$). Les n vecteurs colonnes de M sont les éléments $(a_{1\,j},a_{2\,j},\ldots,a_{m\,j})$ de $\mathbb{K}^m$, $j \in [\![1,n]\!]$.*

Notation 4.3.17 *On note $\mathcal{M}_{(m,\,n)}(\mathbb{K})$ l'ensemble des matrices à coefficients dans $\mathbb{K}$, à m lignes et n colonnes ($m > 0$ et $n > 0$).*

Définition et notation 4.3.18 (Matrice carrée) *Lorsque dans la définition 4.3.14, on a $I = J$, on dit que M est une matrice carrée. On note $\mathcal{M}_n(\mathbb{K})$ l'ensemble des matrices carrées à coefficients dans $\mathbb{K}$ à n lignes et n colonnes.*

Définition 4.3.19 (Rang d'une matrice) *Soit $M \in \mathcal{M}_{(m,\,n)}(\mathbb{K})$. Le rang de M est la dimension du sous-espace de $\mathbb{K}^m$ engendré par les vecteurs colonnes de M. En notant $\operatorname{rg} M$ le rang de M, on a, pour $M = \begin{pmatrix} a_{1\,1} & a_{1\,2} & \cdots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \cdots & a_{2\,n} \\ \vdots & \vdots & & \vdots \\ a_{m\,1} & a_{m\,2} & \cdots & a_{m\,n} \end{pmatrix}$:*

$$\operatorname{rg} M = \dim_{\mathbb{K}}(\operatorname{Vect}_{\mathbb{K}}(C_1, C_2, \ldots, C_n))$$

avec, pour tout $j \in [\![1, n]\!]$, $C_j = (a_{1\,j}, a_{2\,j}, \ldots, a_{m\,j})$.

On constate sans difficulté que la matrice nulle [12] est la seule matrice de $\mathcal{M}_{(m,\,n)}(\mathbb{K})$ de rang zéro, puisque $\dim_{\mathbb{K}}\{0_{\mathbb{K}^m}\} = 0$. Le rang d'une matrice est, d'après des définitions, le rang de la famille formée de ses vecteurs colonnes.

Définition 4.3.20 (Sous-matrice) *Soient I et J des ensembles finis non vides. Soit $M : I \times J \to \mathbb{K}$ une matrice à coefficients dans $\mathbb{K}$. On dit que N est une sous-matrice de M si $N : I' \times J' \to \mathbb{K}$, avec $\emptyset \neq I' \subset I$ et $\emptyset \neq J' \subset J$.*

Théorème 4.3.7 *Soient m et n des nombres entiers strictement positifs. Soit M un élément de $\mathcal{M}_{(m,\,n)}(\mathbb{K})$. Si M n'est pas identiquement nulle, alors le rang r de M est le plus grand des nombres entiers s tel qu'il existe une sous-matrice carrée N de M, $N \in \mathcal{M}_s(\mathbb{K})$, dont le déterminant est différent de zéro.*

Signalons qu'un calcul de déterminant n'est envisageable que sur une matrice carrée.

Démonstration 4.3.7 Montrons que si r est le plus grand des nombres entiers s, tel qu'il existe une sous-matrice de M appartenant à $\mathcal{M}_s(\mathbb{K})$ de déterminant non nul, alors r est le rang de M. Notons N une sous-matrice carrée de M, de "taille maximale" parmi les sous-matrices carrées de M ayant un déterminant non nul. $N \in \mathcal{M}_r(\mathbb{K})$. Notons C'_j, $j \in [\![1, r]\!]$, les vecteurs colonnes de N et C_j, $j \in [\![1, n]\!]$, les vecteurs colonnes de M ; de sorte que pour tout j dans $[\![a, b]\!]$, C_j soit obtenue à partir de C'_j en ajoutant à C'_j un certain nombre de lignes (de composantes). Avec la notation qui vient d'être fixée, C_1 n'est pas nécessairement la première colonne de M, alors que C'_1 est la première colonne de N. Pour tout j dans $[\![1, r]\!]$, C'_j appartient à $\mathbb{K}^r$.

Si $r = m$ alors les m vecteurs colonnes linéairement indépendants de N sont m vecteurs colonnes de M, linéairement indépendants dans $\mathbb{K}^m$. Ces m vecteurs forment donc une base du sous-espace de $\mathbb{K}^m$ qu'ils engendrent ; par conséquent, ces m vecteurs forment une base de $\mathbb{K}^m$. Donc $\operatorname{rg} M = r = m$.

Si $r = n$ alors les vecteurs colonnes de M sont linéairement indépendants, et ils engendrent un sous-espace de $\mathbb{K}^n$ de dimension $r = n$. En effect, si les C_j n'étaient pas linéairement indépendants, alors il existerait des scalaires λ_j, non tous nuls, tels que : $\sum_{j=1}^{n} \lambda_j C_j = 0_{\mathbb{K}^m}$. Mais alors, on aurait : $\sum_{j=1}^{n} \lambda_j C'_j = 0_{\mathbb{K}^n}$, ce qui serait contradictoire avec l'indépendance linéaire des vecteurs colonnes de N.

Si $r < m$ et $r < n$ alors, pour les mêmes raisons que dans le cas $r = n$, la famille $(C_j)_{j \in [\![1,\,r]\!]}$ est libre. Toute sous-matrice de M appartenant à $\mathcal{M}_{r+1}(\mathbb{K})$ a pour déterminant 0. En particulier, si on ajoute une ligne, puis une colonne à N, de sorte à construire une sous-matrice $\check{N}$ de M, $\check{N} \in \mathcal{M}_{r+1}(\mathbb{K})$, on a : $\det \check{N} = 0$. Notons $\check{C}_j$, $j \in [\![1, r]\!] \cup \{k\}$, $r < k \leqslant n$, les vecteurs colonnes de $\check{N}$; de sorte que pour $j \in [\![1, r]\!]$, $\check{C}_j$ soit obtenue en ajoutant une ligne (une composante) à C'_j, et $\check{C}_k$ soit la colonne ajoutée à N' pour former $\check{N}$. $\check{C}_k$ est une sous-matrice de C_k (en considérant les vecteurs colonnes comme des matrices à une colonne). Comme $\det \check{N} = 0$, les vecteurs $\check{C}_j$ sont liés. Il existe donc des scalaires λ_j, non tous nuls, tels que : $\sum_{j \in [\![1,\,r]\!] \cup \{k\}} \lambda_j \check{C}_j = 0_{\mathbb{K}^{r+1}}$. $\lambda_k \neq 0$, car sinon, on aurait $\sum_{j=1}^{r} \lambda_j C'_j = 0_{\mathbb{K}^r}$ avec les λ_j non tous nuls. On a donc : $\check{C}_k = \sum_{j=1}^{r} -\frac{\lambda_j}{\lambda_k} \check{C}_j$. Cette relation induit une relation entre vecteurs de $\mathbb{K}^r$: $C'_k = \sum_{j=1}^{r} -\frac{\lambda_j}{\lambda_k} C'_j$. Or, comme $(C'_j)_{j \in [\![1,\,r]\!]}$ est une base de $\mathbb{K}^r$, les coefficients $-\frac{\lambda_j}{\lambda_k}$ sont uniquement déterminés. D'autre part, C'_k ne dépend pas de la ligne ajoutée à N pour former $\check{N}$, mais dépend seulement de la colonne ajoutée à N. On aura donc, pour toute sous-matrice $\check{C}_k$ de C_k, les même scalaires $-\frac{\lambda_j}{\lambda_k}$ tels que : $\check{C}_k = \sum_{j=1}^{r} -\frac{\lambda_j}{\lambda_k} \check{C}_j$. D'où $C_k = \sum_{j=1}^{r} -\frac{\lambda_j}{\lambda_k} C_j$, et donc $C_k \in \operatorname{Vect}_{\mathbb{K}}(C_1, C_2, \ldots, C_r)$. La démonstration de

12. $M : [\![1, m]\!] \times [\![1, n]\!] \to \mathbb{K}$ est la matrice nulle si, pour tout (i, j) dans $I \times J$, l'image de (i, j) par M est l'élément 0 de $\mathbb{K}$.

l'appartenance de C_k à $\mathrm{Vect}_{\mathbb{K}}(C_1,C_2,\ldots,C_r)$ est valable pour tout $k \in [\![r+1,n]\!]$. On en déduit que le sous-espace de $\mathbb{K}^m$ engendré par les vecteurs colonnes de M est $\mathrm{Vect}_{\mathbb{K}}(C_j)_{j\in[\![1,r]\!]}$, dont $(C_j)_{j\in[\![1,r]\!]}$ est une base. D'où $\mathrm{rg}\, M = r$.

Supposons $\mathrm{rg}\, M = r$. Comme M n'est pas la matrice nulle, $r \neq 0$ et il existe une sous-matrice de M de déterminant non nul. Or, d'après la première partie de la démonstration, le plus grand des nombres entiers s tel qu'il existe une sous-matrice N de M, $N \in \mathcal{M}_s(\mathbb{K})$ $\det N \neq 0$, est le rang de M. On en déduit que la plus grande sous-matrice carrée (les plus grandes sous-matrices carrées) de M de déterminant non nul est un élément (sont des éléments) de $\mathcal{M}_r(\mathbb{K})$.

Définition et notation 4.3.21 (transposée) *Soit M un élément de $\mathcal{M}_{(m,n)}(\mathbb{K})$. La transposée de M, notée : ${}^tM$, est l'élément de $\mathcal{M}_{(n,m)}(\mathbb{K})$ défini pour tout (j,i) dans $[\![1,n]\!]\times[\![1,m]\!]$, par : ${}^tM(j,i) = M(i,j)$.*

Comme nous savons que le déterminant d'une matrice carrée est égal à celui de sa transposée, nous pouvons déduire du théorème 4.3.7 :

Corollaire 4.3.7.1 *Soit M un élément de $\mathcal{M}_{(m,n)}(\mathbb{K})$. Le rang de M est la dimension du sous-espace vectoriel de $\mathbb{K}^n$ engendré par les vecteurs lignes de M. Autrement dit, si $M = \begin{pmatrix} a_{1\,1} & a_{1\,2} & \cdots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \cdots & a_{2\,n} \\ \vdots & \vdots & & \vdots \\ a_{m\,1} & a_{m\,2} & \cdots & a_{m\,n} \end{pmatrix}$, alors $\mathrm{rg}\, M = \dim_{\mathbb{K}}(\mathrm{Vect}_{\mathbb{K}}(L_1,L_2,\ldots,L_m))$, avec $L_i = (a_{i\,1},a_{i\,2},\ldots,a_{i\,n}) \in \mathbb{K}^n$ pour tout i dans $[\![1,m]\!]$*

Le rang d'une matrice est donc le rang commun de la famille de ses vecteurs colonnes et de la famille de ses vecteurs lignes.

Corollaire 4.3.7.2 *Pour toute matrice M de $\mathcal{M}_{(m,n)}(\mathbb{K})$:*

$$\mathrm{rg}\, M = \mathrm{rg}\, {}^tM.$$

Corollaire 4.3.7.3 *Soit M un élément de $\mathcal{M}_{(m,n)}(\mathbb{K})$. Soit N l'élément de $\mathcal{M}_{(m,n)}(\mathbb{K})$ obtenu à partir de M en effectuant une des opérations suivantes :*

- *ajout, à une ligne de M, d'une combinaison linéaire des autres lignes de M ;*
- *ajout, à une colonne de M, d'une combinaison linéaire des autres colonnes de M ;*
- *échange de deux lignes ;*
- *échange de deux colonnes.*

Alors, on a : $\mathrm{rg}\, N = \mathrm{rg}\, M$.

Démonstration 4.3.7.3 Ce corollaire est une conséquence triviale du théorème 4.3.7, de la proposition 4.2.4 page 42, et de la propriété d'antisymétrie du déterminant.

Définition 4.3.22 (Rang d'un système) *Considérons le systèmes (S) de m équations linéaires à n inconnues $x_1,\ldots,x_n$:*

$$(S) \quad \begin{cases} a_{1\,1}x_1 & + & \cdots & + & a_{1\,n}x_n & = & b_1 \\ \vdots & & \vdots & & \vdots & \vdots & \vdots \\ a_{m\,1}x_1 & + & \cdots & + & a_{m\,n}x_n & = & b_m \end{cases}$$

Le rang du système (S) est alors celui de la matrice $M = \left(a_{i\,j}\right)_{(i,j)\in[\![1,m]\!]\times[\![1,n]\!]}$.

4.4 Pivot de Gauss

Nous allons aborder une technique permettant de déterminer le rang d'un système, d'une matrice, mais aussi de résoudre un système d'équations linéaires. Cette technique est appelée « combinaison », pour les systèmes d'équations, lorsqu'elle est abordée dans les classes du secondaire.

4.4.1 Détermination du rang d'une matrice

Théorème 4.4.1 *Soit M un élément de $\mathcal{M}_{(m,\,n)}(\mathbb{K})$, $m > 1$ et $n > 1$. Si M n'est pas la matrice nulle, alors il existe une matrice N appartenant à $\mathcal{M}_{(m,\,n)}(\mathbb{K})$, telle que :*

1. *M et N sont de même rang ;*
2. $N = \left(\begin{array}{c|c} \lambda & \cdots \\ \hline 0 & \\ \vdots & N' \\ 0 & \end{array}\right)$, $\lambda \neq 0$, $N' \in \mathcal{M}_{(m-1,\,n-1)}(\mathbb{K})$ *et* $\operatorname{rg} N = 1 + \operatorname{rg} N'$.

Démonstration 4.4.1 Si M n'est pas la matrice nulle de $\mathcal{M}_{(m,\,n)}(\mathbb{K})$, alors il existe au moins un coefficient de M, disons $a_{i_0\,j_0}$, non nul. À partir de M, en échangeant la ligne 1 et avec la ligne i_0, puis la colonne 1 et avec la colonne j_0, on obtient une matrice $M' = \left(m_{i\,j}\right)_{(i,\,j)\in[\![1,\,m]\!]\times[\![1,\,n]\!]}$ de même rang que M (voir le corollaire 4.3.7.3). Posons $\lambda = a_{i_0\,j_0} = m_{1\,1}$. Pour tout i dans $[\![2, m]\!]$, ajoutons à la ligne i de M', $-\frac{m_{i\,1}}{\lambda}$ fois la première ligne de M'. On obtient alors une matrice $N = \left(\begin{array}{c|c} \lambda & \cdots \\ \hline 0 & \\ \vdots & N' \\ 0 & \end{array}\right)$, dont toutes les lignes, sauf la première, commencent par 0. Cette matrice est de même rang que M (corollaire 4.3.7.3). Les matrices N' et $N'' = \left(\begin{array}{c|c} 0 & \\ \vdots & N' \\ 0 & \end{array}\right) \in \mathcal{M}_{(m-1,\,n)}(\mathbb{K})$ sont de même rang, car le nombre de vecteurs colonnes linéairement indépendants est le même pour N' et pour N''. Puisque tous les vecteurs lignes de N'' ont pour première composante 0, et comme $\lambda \neq 0$, $\operatorname{rg} N = 1 + \operatorname{rg} N''$; on en déduit : $\operatorname{rg} N = 1 + \operatorname{rg} N'$.

Notons que si dans le $M \in \mathcal{M}_{(1,\,n)}(\mathbb{K})$ et si M est non nulle, alors $\operatorname{rg} M = 1$. De même, si $M \in \mathcal{M}_{(m,\,1)}(\mathbb{K})$ et si M est non nulle, alors $\operatorname{rg} M = 1$; 1 est également le rang des matrices $\begin{pmatrix} \lambda \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathcal{M}_{(m,\,1)}(\mathbb{K})$ et $\begin{pmatrix} \lambda & \cdots \end{pmatrix} \in \mathcal{M}_{(1,\,n)}(\mathbb{K})$, si $\lambda \neq 0$.

Définition 4.4.1 (Pivot) *Le coefficient λ avec lequel on travaille dans la démonstration du théorème 4.4.1 s'appelle le pivot.*

Corollaire 4.4.1.1 *Soit M un élément de $\mathcal{M}_{(m,\,n)}(\mathbb{K})$. Si M n'est pas la matrice nulle, alors il existe une matrice carrée triangulaire supérieure : $T \in \mathcal{M}_r(\mathbb{K})$, $0 < r \leqslant \max\{m, n\}$, dont tous les coefficients diagonaux sont différents de 0, telle que la matrice $\check{M} \in \mathcal{M}_{(m,\,n)}(\mathbb{K})$, vérifie :*

$$\check{M} = \left(\begin{array}{ccc|ccc} \multicolumn{3}{c|}{T} & \multicolumn{3}{c}{\cdots} \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right), \text{ et}$$

$$\operatorname{rg} M = \operatorname{rg} \check{M}.$$

Démonstration 4.4.1 Si $m = 1$ ou $n = 1$, il suffit d'utiliser encore une fois le corollaire 4.3.7.3 pour donner à $\check{M}$ l'aspect voulu. Sinon, il suffit d'utiliser, plusieurs fois de suite si nécessaire, le théorème 4.4.1 en remplaçant N par N' à chaque fois. Ce processus s'arrête quand N' n'a plus qu'une ligne, ou quand tous les coefficients de N' sont nuls. Quand N' n'a plus qu'une colonne et n'est pas la matrice nulle, on utilise un coefficient de N' comme pivot, de sorte à remplacer N' par une matrice de type : $\begin{pmatrix} \mu \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, et le processus s'arrête.

On remarque que lorsqu'il faut échanger des lignes ou des colonnes dans le bloc N' afin de parvenir à la forme de matrice voulue, on peut échanger les lignes ou les colonnes correspondantes dans N, sans perturber le bloc

triangulaire déjà obtenu à ce stade. On remarque également que les deux blocs de zéros peuvent ne pas apparaître ; autrement dit : on peut obtenir une matrice $\check{M}$ de type : T, $\left(\begin{array}{c|c} T & \cdots \end{array}\right)$ ou $\left(\begin{array}{c} T \\ \hline 0 \ \cdots \ 0 \\ \vdots \quad \vdots \\ 0 \ \cdots \ 0 \end{array}\right)$.

Exemples :

a. Considérons la matrice $M_a = \begin{pmatrix} 2 & 3 & 0 \\ 4 & -1 & -1 \end{pmatrix}$. M_a et $\check{M}_a = \begin{pmatrix} 2 & 3 & 0 \\ 0 & -7 & -1 \end{pmatrix}$ obtenue en ajoutant -2 fois la ligne 1 à la ligne 2 de M_a, sont de même rang ; dans cette étape de calcul, le pivot est 2. $\check{M}_a$ a bien la forme annoncée dans le corollaire, en posant $T_a = \begin{pmatrix} 2 & 3 \\ 0 & -7 \end{pmatrix}$. (On est dans le cas où le processus s'arrête lorsque N' n'a plus qu'une ligne).

b. Considérons $M_b = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$. Commençons par échanger les colonnes 1 et 2 de M_b. On obtient $M'_b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix}$. On se sert ensuite du premier coefficient de la première ligne : 1, comme pivot. En combinant les autres lignes avec la première ligne, on obtient $M''_b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix} \begin{array}{lll} L_1 & & \\ L_2 & \longleftarrow & L_2 \\ L_3 & \longleftarrow & L_3 - L_1 \\ L_4 & \longleftarrow & L_4 \end{array}$. On échange les colonnes 2 et 3. On obtient $M'''_b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 0 \end{pmatrix} \begin{array}{l} L_1 \\ L_2 \\ L_3 \\ L_4 \end{array}$. Le nouveau pivot est le coefficient 1 qui se trouve en deuxième ligne deuxième colonne. $\check{M}_b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{array}{lll} L_1 & & \\ L_2 & & \\ L_3 & \longleftarrow & L_3 - L_2 \\ L_4 & \longleftarrow & L_4 - 2L_2 \end{array}$. $\operatorname{rg} M_b = \operatorname{rg} \check{M}_b$.

Proposition 4.4.2 *Soit $\check{M}$ un élément de $\mathcal{M}_{(m,\,n)}(\mathbb{K})$. S'il existe une matrice triangulaire supérieure $T \in \mathcal{M}_r(\mathbb{K})$, $r \geqslant 1$, dont tous les coefficients diagonaux sont différents de zéro, et telle que :*

$$\check{M} = \left(\begin{array}{ccc|ccc} \multicolumn{3}{c|}{T} & \multicolumn{3}{c}{\cdots} \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right),$$

alors,

$$\operatorname{rg} \check{M} = \operatorname{rg} T = r.$$

Démonstration 4.4.2 Pour montrer que $\operatorname{rg} T = r$, il suffit de prouver que le déterminant de T n'est pas égal à zéro. Or, d'après le corollaire 4.3.5.1, le déterminant de T est le produit de ses termes diagonaux. Les termes diagonaux de T étant tous non nuls, $\det T \neq 0$ et donc : $\operatorname{rg} T = r$. Le fait que $\operatorname{rg} \check{M} = \operatorname{rg} T$ est une conséquence directe du théorème 4.3.7 et de la forme de $\check{M}$.

En appliquant la proposition 4.4.2 aux matrices M_a et M_b des exemples ci-dessus, on obtient : $\operatorname{rg} M_a = 2$ et $\operatorname{rg} M_b = 2$. La méthode consistant à transformer une matrice M en une matrice de même rang : $\check{M}$ (comme dans le corollaire 4.4.1.1), dont on sait déterminer le rang (via le corollaire 4.4.1.1 et la proposition 4.4.2), s'appelle : la méthode du **pivot de Gauss**. Quand une matrice A se présente sous une forme du type de celle de la matrice $\check{M}$ de la proposition 4.4.2, on dit parfois que A est **échelonnée**. Il est fortement recommandé d'utiliser la méthode (simple) du pivot de Gauss pour déterminer le rang d'une matrice.

4.4.2 Résolution d'un système d'équations linéaires

Soient m et n des nombres entiers naturels différents de zéro. Soient $a_{i\,j} \in \mathbb{K}$ pour $i \in [\![1, m]\!]$ et $j \in [\![1, n]\!]$. Soit $(b_1, b_2, \ldots, b_m) \in \mathbb{K}^m$. Considérons le système (S) de m équations linéaires à n inconnues $x_1, \ldots, x_n$:

$$(S) \quad \left\{ \begin{array}{ccccccccc} a_{1\,1}x_1 & + & a_{1\,2}x_2 & + & \cdots & + & a_{1\,n}x_n & = & b_1 \\ a_{2\,1}x_1 & + & a_{2\,2}x_2 & + & \cdots & + & a_{2\,n}x_n & = & b_2 \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ a_{m\,1}x_1 & + & a_{m\,2}x_2 & + & \cdots & + & a_{m\,n}x_n & = & b_m \end{array} \right.$$

Dans le cas où tous les coefficients $a_{i\,j}$ sont nuls, ou bien $b_1 = \cdots = b_m = 0$ et l'ensemble des solutions est $\mathbb{K}^n$, ou bien au moins un des b_i est différent de 0 et dans ce cas l'ensemble des solutions est $\emptyset$. Dans le où au moins un des $a_{i\,j}$ est différent de 0, on définit alors la matrice M du système par :

$$M = \Big(a_{i\,j}\Big)_{(i,\,j) \in [\![1,\,m]\!] \times [\![1,\,n]\!]}.$$

Puis on définit la matrice $\hat{M}$ par : $\hat{M} = \left(\begin{array}{c|c} M & B \end{array}\right)$, où B désigne la matrice $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$. La méthode du pivot de Gauss consiste alors à transformer M en une matrice du type « $\check{M}$ » (voir la sous-section précédente), mais en travaillant sur $\hat{M}$, et en répercutant ainsi toutes les opérations effectuées sur les lignes, sur la dernière colonne B de $\hat{M}$. Après un certain nombre d'opérations (celles exposées dans la démonstration du corollaire 4.4.1.1), on obtient une matrice $\check{\hat{M}} = \left(\begin{array}{c|c} \check{M} & \mathfrak{B} \end{array}\right) = \left(\begin{array}{ccc|ccc|c} \multicolumn{3}{c|}{T} & \multicolumn{3}{c|}{\cdots} & \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 & \\ \vdots & & \vdots & \vdots & & \vdots & \mathfrak{B} \\ 0 & \cdots & 0 & 0 & \cdots & 0 & \end{array}\right)$, $T \in \mathcal{M}_r(\mathbb{K})$ triangulaire supérieure, $\det T \neq 0$, $\mathfrak{B}$ étant obtenue à partir de B en effectuant sur B les opérations effectuées sur les lignes de M pour obtenir $\check{M}$. $\check{\hat{M}}$ correspond à un système (S') équivalent au système (S). Le terme de **système échelonné** est parfois utilisé pour désigner un système tel que (S').

Exemple

Considérons le système : (S_a) $\left\{ \begin{array}{cccc} 2x & +3y & = & 2 \\ 4x & -y \quad -z & = & 5 \end{array} \right.$ et résolvons ce système dans $\mathbb{K}^3$ en utilisant la méthode du pivot de Gauss. On remarque que la matrice du système est la matrice M_a donnée page 55. Le système (S_a) est représenté par la matrice :

$$\hat{M}_a = \left(\begin{array}{ccc|c} 2 & 3 & 0 & 2 \\ 4 & -1 & -1 & 5 \end{array}\right).$$

(S_a) est équivalent au système (S'_a), correspondant à la matrice :

$$\check{\hat{M}}_a = \left(\begin{array}{ccc|c} 2 & 3 & 0 & 2 \\ 0 & -7 & -1 & 1 \end{array}\right).$$

Donc, (S'_a) $\left\{ \begin{array}{cccc} 2x & 3y & = & 2 \\ & -7y \quad -z & = & 1 \end{array} \right.$. Les solutions de (S_a), qui sont également les solutions de (S'_a), sont les éléments $\left(-\frac{3}{2}y + 1, y, -7y - 1\right)$ de $\mathbb{K}^3$, $y \in \mathbb{K}$. L'ensemble des solutions de (S_a) est un sous-espace affine [13] de $\mathbb{K}^3$; c'est le sous-espace affine : $(1, 0, -1) + \mathbb{K}\left(-\frac{3}{2}, 1, -7\right)$, qui a comme sous-espace vectoriel directeur, le sous-espace de dimension 1 : $\mathrm{Vect}_{\mathbb{K}}\left(\left(-\frac{3}{2}, 2, -7\right)\right)$.

Notons pour terminer, que si lors de la résolution du système, on obtient une égalité de type : « $0 = 0$ », alors, cette égalité étant vraie quelles que soient les valeurs attribuées aux inconnues du système, on peut tout simplement supprimer cette égalité du système tout en conservant un système équivalent. Si c'est une égalité de type : « $1 = 0$ » qui apparaît, alors le système n'a pas de solution.

13. La notion d'espace affine n'est pas au programme du premier semestre.

Annexe A

Fractions rationnelles

La notation $\mathbb{K}$ peut être remplacée indifféremment par $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.
Nous avons constaté, dans le chapitre sur les polynômes, que les seuls polynômes ayant un inverse (pour le produit défini sur $\mathbb{K}[X]$) sont ceux de degré 0 ; les polynômes de degré 0 étant les éléments de $\mathbb{K}^*$. Ce qui est vrai dans $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, à savoir : « tout élément non nul possède un inverse (pour le produit habituel sur ces ensembles de nombres) », n'est vrai ni dans $\mathbb{Z}$, ni dans $\mathbb{K}[X]$. Nous allons examiner ici une construction, similaire à celle permettant de passer de $\mathbb{Z}$ à $\mathbb{Q}$, du corps des fractions rationnelles à une indéterminée [1]. La construction envisagée ici utilise les notions de relation d'équivalence et de classes d'équivalence. Si de telles notions vous semblent un peu trop exotiques, et si vous savez quel sens donner à $\frac{a}{b}$ pour a et b entiers relatifs ($b \neq 0$), alors vous devinerez parfaitement la signification de $\frac{P}{Q}$ pour P et Q dans $\mathbb{K}[X]$ et vous pourrez aller directement à la partie : décomposition en éléments simples.

A.1 L'ensemble $\mathbb{K}(X)$

A.1.1 Une construction de $\mathbb{K}(X)$

Complément sur les ensembles

Définition A.1.1 (Relation d'équivalence) *Soit $\mathcal{E}$ un ensemble. On dit que $\mathcal{R}$, $\mathcal{R} \subset \mathcal{E} \times \mathcal{E}$, est une relation d'équivalence sur $\mathcal{E}$ si :*

1. *pour tout a dans $\mathcal{E}$: $(a, a) \in \mathcal{R}$ (la relation est réflexive),*
2. *pour tout a et tout b dans $\mathcal{E}$: si $(a, b) \in \mathcal{R}$ alors $(b, a) \in \mathcal{R}$ (la relation est symétrique),*
3. *pour tout a, tout b et tout c dans $\mathcal{E}$: si $(a, b) \in \mathcal{R}$ et $(b, c) \in \mathcal{R}$ alors $(a, c) \in \mathcal{R}$ (la relation est transitive).*

L'égalité, sur n'importe quel ensemble, est une relation d'équivalence (preuve?).

Exercice A.1.1 *Soit $\mathcal{E}$ un ensemble non vide. Soit la famille $(\mathcal{A}_i)_{i\in I}$ de sous-ensembles de $\mathcal{E}$ vérifiant :*

$$(\forall i \in I)(\forall j \in I) \quad i \neq j \Rightarrow \mathcal{A}_i \cap \mathcal{A}_j = \emptyset,$$

$$\mathcal{E} = \bigcup_{i\in I} \mathcal{A}_i.$$

On dit dans ce cas que $(\mathcal{A}_i)_{i\in I}$ est une partition de $\mathcal{E}$. On considère la relation $\mathcal{R}$, $\mathcal{R} \subset \mathcal{E} \times \mathcal{E}$, définie par :

$$(a, b) \in \mathcal{R} \iff (\exists i_0 \in I) \quad a \in \mathcal{A}_{i_0} \text{ et } b \in \mathcal{A}_{i_0}.$$

Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathcal{E}$.

Définition A.1.2 (Classe d'équivalence) *Soit $\mathcal{E}$ un ensemble, et soit $\mathcal{R}$ une relation d'équivalence sur $\mathcal{E}$. Pour tout x dans $\mathcal{E}$, la classe d'équivalence de x est l'ensemble des éléments y de $\mathcal{E}$ tels que $(x, y) \in \mathcal{R}$.*

1. On dit aussi : fractions rationnelles à une variable, ou encore : fractions rationnelles.

Une relation d'équivalence sur $\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$

Première tentative :

Considérons la relation $\mathcal{R} \subset (\mathbb{K}[X]\times\mathbb{K}[X])\times(\mathbb{K}[X]\times\mathbb{K}[X])$ définie par : $((P,Q),(R,S)) \in \mathcal{R} \iff PS = RQ$. Malheureusement, $\mathcal{R}$ ainsi définie n'est pas une relation d'équivalence. Notre ambition était, au cas où $\mathcal{R}$ aurait été une relation d'équivalence, de noter $\frac{P}{Q}$ la classe d'équivalence de (P,Q). On aurait alors eu : $\frac{P}{Q} = \frac{R}{S} \iff PS = RQ$. Examinons de plus près le défaut de notre définition de $\mathcal{R}$. D'après la définition de $\mathcal{R}$, pour tout $(P,Q) \in \mathbb{K}[X]\times\mathbb{K}[X]$: $((P,Q),(0,0)) \in \mathcal{R}$. Autrement écrit : « $\frac{P}{Q} = \frac{0}{0}$ ». Mais alors, on a : « $\frac{0}{0} = \frac{1}{2}$ », « $\frac{0}{0} = \frac{2}{1}$ » et « $\frac{2}{1} \neq \frac{1}{2}$ » ; la transitivité est mise en défaut. L'erreur commise pour définir $\mathcal{R}$ est celle que quelques jeunes gens commetttent lorsqu'ils sont confrontés pour la première fois aux fractions : accepter la valeur 0 au dénominateur.

Seconde tentative :

Proposition A.1.1 *On considère la relation* $\mathcal{R} \subset (\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})) \times (\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\}))$ *définie par :* $((P,Q),(R,S)) \in \mathcal{R} \iff PS = RQ$. $\mathcal{R}$ *est une relation d'équivalence.*

Démonstration A.1.1 Exercice.

Définitions et notations A.1.3 ($\frac{P}{Q}$**,** $\mathbb{K}(X)$**)** *Notons* [2] $\frac{P}{Q}$ *la classe d'équivalence, pour la relation d'équivalence* $\mathcal{R}$ *définie dans la proposition A.1.1, de* (P,Q)*, élément de* $\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$*. L'ensemble des classes d'équivalence* $\frac{P}{Q}$ *est noté* $\mathbb{K}(X)$*.* $\mathbb{K}(X)$ *est l'ensemble des fractions rationnelles.*

Exercice A.1.2 *Montrer que pour tout* $(P,Q) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$ *et tout* $R \in \mathbb{K}[X] \setminus \{0\}$*, on a :*

$$\frac{P}{Q} = \frac{PR}{QR}.$$

A.1.2 Un produit et une somme sur $\mathbb{K}(X)$

Exercice A.1.3 *On considère les fractions rationnelles* $\frac{P_0}{Q_0}$, $\frac{R_0}{S_0}$, $\frac{P_1}{Q_1}$ *et* $\frac{R_1}{S_1}$.
Montrer que si $\frac{P_0}{Q_0} = \frac{P_1}{Q_1}$ *et* $\frac{R_0}{S_0} = \frac{R_1}{S_1}$ *alors :*

1. $\frac{P_0R_0}{Q_0S_0} = \frac{P_1R_1}{Q_1S_1}$
2. $\frac{P_0S_0+R_0Q_0}{Q_0S_0} = \frac{P_1S_1+R_1Q_1}{Q_1S_1}$

Les résultats de l'exercice A.1.3 vont nous permettre de définir le produit et la somme d'éléments de $\mathbb{K}(X)$, en utilisant des représentants [3] des classes d'équivalence, puisque ces définitions seront indépendante du choix des représentants.

Définition A.1.4 (Multiplication) *Soient* $\frac{P}{Q}$ *et* $\frac{R}{S}$ *des éléments de* $\mathbb{K}(X)$*. Le produit* $\frac{P}{Q}\frac{R}{S}$ *de ces éléments est défini par :*

$$\frac{P}{Q}\frac{R}{S} = \frac{PR}{QS}.$$

Le produit ainsi défini est bien défini ; i.e. *la définition du produit ne dépendant pas des polynômes* P*,* Q*,* R *et* S*, mais seulement des classes d'équivalence des couples* (P,Q) *et* (R,S)*.*

Définition A.1.5 (Addition) *Soient* $\frac{P}{Q}$ *et* $\frac{R}{S}$ *des éléments de* $\mathbb{K}(X)$*. La somme* $\frac{P}{Q} + \frac{R}{S}$ *de ces éléments est définie par :*

$$\frac{P}{Q} + \frac{R}{S} = \frac{PS + RQ}{QS}.$$

La somme ainsi définie est bien définie ; i.e. *la définition de la somme ne dépendant pas des polynômes* P*,* Q*,* R *et* S*, mais seulement des classes d'équivalence des couples* (P,Q) *et* (R,S)*.*

Exercice A.1.4 *Vérifier que le produit et la somme ainsi définis sont des lois internes associatives et commutatives, que* $\frac{0}{1}$ *est l'élément neutre de la somme,* $\frac{1}{1}$ *celui du produit, que la multiplication est distributive par rapport à l'addition, que* $\frac{P}{Q}$ *a pour opposé* $\frac{-P}{Q}$*, que* $\frac{P}{Q}$*,* $Q \neq 0$*, a pour inverse* $\frac{Q}{P}$*.*

2. $\frac{P}{Q}$ se lit... « P sur Q ». Etonnant, non ?
3. Des polynômes.

A.1.3 Une injection de $\mathbb{K}[X]$ dans $\mathbb{K}(X)$

Considérons l'application $f : \mathbb{K}[X] \to \mathbb{K}(X)$ définie [4] par $f(P) = \frac{P}{1}$.

Proposition A.1.2 *f est injective.*

Démonstration A.1.2 $f(P) = f(Q) \iff \frac{P}{1} = \frac{Q}{1} \iff 1P = 1Q \iff P = Q$.

Proposition A.1.3 *Pour tout P et tout Q dans $\mathbb{K}[X]$:*

$$f(P+Q) = f(P) + f(Q),$$

$$f(PQ) = f(P)f(Q).$$

Démonstration A.1.3 $f(P+Q) = \frac{P+Q}{1} = \frac{1P+1Q}{1\times 1} = \frac{P}{1} + \frac{Q}{1} = f(P) + f(Q)$, $f(PQ) = \frac{PQ}{1} = \frac{PQ}{1\times 1} = \frac{P}{1}\frac{Q}{1} = f(P)f(Q)$.

Comme dans le cas des nombres complexes, comme dans le cas des polynômes, les notations vont être simplifiées. On identifie $\mathbb{K}[X]$ à sont image par f ; ce qui induit la simplification d'écriture : $\frac{P}{1} = P$ pour tout $P \in \mathbb{K}[X]$. On écrira $-\frac{P}{Q}$ de préférence à $\frac{-P}{Q}$. Pour $Q \neq 0$, « P divisé par Q » signifie : « $\frac{P}{1}$ multiplié par $\frac{1}{Q}$ »...

$\mathbb{K}(X)$ muni des deux lois internes produit et somme définies ci-dessus est un corps commutatif.

A.2 Décomposition en éléments simples

Théorème A.2.1 (Décomposition en éléments simples) *Soient A et B de éléments de $\mathbb{K}[X]$, $B \neq 0$, et soit $\lambda {P_1}^{r_1} {P_2}^{r_2} \cdots {P_m}^{r_m}$ la décomposition de B en produit d'un élément de $\mathbb{K}^*$: λ, et de facteurs irréductibles et unitaires dans $\mathbb{K}[K]$, telle que pour tout i et tout j dans $[\![1,m]\!]$, $i \neq j \Rightarrow P_i \neq P_j$, et pour tout i dans $[\![1,m]\!]$, $r_i > 0$. Alors, il existe $Q \in \mathbb{K}[X]$, pour tout $i \in [\![1,m]\!]$, il existe des éléments $A_{i\,1}$, $A_{i\,2}, \cdots$, $A_{i\,r_i}$ de $\mathbb{K}[X]$, tels que :*

$$\frac{A}{B} = Q + \sum_{i=1}^{m} \left(\sum_{j=1}^{r_i} \frac{A_{i\,j}}{{P_i}^j} \right) \tag{A.1}$$

et

$$(\forall i \in [\![1,m]\!])(\forall j \in [\![1,r_i]\!]) \quad \deg A_{i\,j} < \deg P_i \tag{A.2}$$

Q, ainsi que les $A_{i\,j}$, sont déterminés de manière unique. $Q + \sum_{i=1}^{m} \left(\sum_{j=1}^{r_i} \frac{A_{i\,j}}{{P_i}^j} \right)$ est la décomposition en éléments simples de la fraction $\frac{A}{B}$.

Pour une meilleure digestion de la démonstration, celle-ci a été découpée en tranches...

Lemme A.2.1.1 *Soient A et B des éléments de $\mathbb{K}[X] \setminus \{0\}$ premiers entre eux. Alors, il existe U et V dans $\mathbb{K}[X]$ tels que :*

$$\frac{1}{AB} = \frac{V}{A} + \frac{U}{B}.$$

Démonstration A.2.1.1 D'après le théorème de Bezout, page 29, puisque A et B sont premiers entre eux, il existe des polynômes U et V tels que $AU + BV = 1$. Il ne reste plus qu'à considérer cette égalité comme une égalité non plus entre éléments de $\mathbb{K}[X]$, mais comme une égalité entre éléments de $\mathbb{K}(X)$, puis à multiplier chacun des membres de cette égalité par $\frac{1}{AB}$; autrement dit : diviser par AB.

Lemme A.2.1.2 *Soient A et B de éléments de $\mathbb{K}[X]$, $B \neq 0$, et soit $\lambda {P_1}^{r_1} {P_2}^{r_2} \cdots {P_m}^{r_m}$ la décomposition de B en produit d'un élément de $\mathbb{K}^*$: λ, et de facteurs irréductibles et unitaires dans $\mathbb{K}[K]$, telle que pour tout i et tout j dans $[\![1,m]\!]$, $i \neq j \Rightarrow P_i \neq P_j$, et pour tout i dans $[\![1,m]\!]$, $r_i > 0$. Alors, il existe A_1, $A_2, \cdots$, A_m dans $\mathbb{K}[X]$ tels que :*

$$\frac{A}{B} = \sum_{i=1}^{m} \frac{A_i}{{P_i}^{r_i}}.$$

Et si $\frac{A}{B} = \sum_{i=1}^{m} \frac{\tilde{A}_i}{{P_i}^{r_i}}$, alors pour tout $i \in [\![1,m]\!]$, $A_i - \tilde{A}_i \in ({P_i}^{r_i})$.

4. On rappelle que $1 = X^0$ (voir page 25).

Démonstration A.2.1.2 L'existence des A_i est une conséquence évidente du lemme A.2.1.1. Si $\sum_{i=1}^m \frac{A_i}{{P_i}^{r_i}} = \sum_{i=1}^m \frac{\tilde{A}_i}{{P_i}^{r_i}}$, alors $(A_j - \tilde{A}_j)\prod_{\substack{i=1\\i\neq j}}^m {P_i}^{r_i} = {P_j}^{r_j}\prod_{\substack{i=1\\i\neq j}}^m {P_i}^{r_i}\left(\sum_{\substack{i=1\\i\neq j}}^m \frac{\tilde{A}_i - A_i}{{P_i}^{r_i}}\right)$. Or, $\prod_{\substack{i=1\\i\neq j}}^m {P_i}^{r_i}\left(\sum_{\substack{i=1\\i\neq j}}^m \frac{\tilde{A}_i - A_i}{{P_i}^{r_i}}\right)$ appartient à $\mathbb{K}[X]$. On en déduit que ${P_j}^{r_j}$ divise $(A_j - \tilde{A}_j)\prod_{\substack{i=1\\i\neq j}}^m {P_i}^{r_i}$. Comme ${P_j}^{r_j}$ et $\prod_{\substack{i=1\\i\neq j}}^m {P_i}^{r_i}$ sont premiers entre eux (preuve?), le théorème de Gauss (page 29) implique que ${P_j}^{r_j}$ divise $A_j - \tilde{A}_j$; autrement dit : $A_j - \tilde{A}_j \in ({P_j}^{r_j})$.

Lemme A.2.1.3 *Pour tout $(A, B) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$, il existe un unique $(Q, R) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tel que :*

$$\frac{A}{B} = Q + \frac{R}{B} \text{ et } \deg R < \deg B.$$

Démonstration A.2.1.3 Il suffit d'utiliser le théorème 3.2.2 page 26.

Lemme A.2.1.4 *Soient A et B de éléments de $\mathbb{K}[X]$, $B \neq 0$, et soit $\lambda {P_1}^{r_1}{P_2}^{r_2}\cdots{P_m}^{r_m}$ la décomposition de B en produit d'un élément de $\mathbb{K}^*$: λ, et de facteurs irréductibles et unitaires dans $\mathbb{K}[K]$, telle que pour tout i et tout j dans $[\![1, m]\!]$, $i \neq j \Rightarrow P_i \neq P_j$, et pour tout i dans $[\![1, m]\!]$, $r_i > 0$. Alors, il existe Q, R_1, $R_2, \cdots, R_m$ dans $\mathbb{K}[X]$, uniquement déterminés, tels que :*

$$\frac{A}{B} = Q + \sum_{i=1}^m \frac{R_i}{{P_i}^{r_i}} \tag{A.3}$$

et

$$(\forall i \in [\![1, m]\!]) \quad \deg R_i < \deg {P_i}^{r_i} \tag{A.4}$$

Démonstration A.2.1.4 D'après le lemme A.2.1.2, il existe A_1, $A_2, \cdots, A_m$ dans $\mathbb{K}[X]$ tels que $\frac{A}{B} = \sum_{i=1}^m \frac{A_i}{{P_i}^{r_i}}$. En appliquant le lemme A.2.1.3 à chaque $\frac{A_i}{{P_i}^{r_i}}$, on obtient pour tout i dans$[\![1, m]\!]$, l'existence de Q_i et R_i dans $\mathbb{K}[X]$, tels que $\frac{A_i}{{P_i}^{r_i}} = Q_i + \frac{R_i}{{P_i}^{r_i}}$ et $\deg R_i < \deg {P_i}^{r_i}$. D'où, en posant $Q = \sum_{i=1}^m Q_i$, on a : $\frac{A}{B} = Q + \sum_{i=1}^m \frac{R_i}{{P_i}^{r_i}}$, avec $\deg R_i < \deg {P_i}^{r_i}$.

Montrons l'unicité des polynômes Q, $R_1, \cdots, R_m$. Supposons qu'il existe dans $\mathbb{K}[X]$, Q, $R_1, \cdots, R_m$ d'une part, $\tilde{Q}$, $\tilde{R}_1, \cdots, \tilde{R}_m$ d'autre part, vérifiant A.3 et A.4. On obtient, exactement comme dans la démonstration du lemme A.2.1.2, que $R_i - \tilde{R}_i \in ({P_i}^{r_i})$. Or, $\deg R_i - \tilde{R}_i \leqslant \max\{\deg R_i, \deg \tilde{R}_i\} < \deg {P_i}^{r_i}$. D'où, $R_i - \tilde{R}_i = 0$. Comme pour tout $i \in [\![1, m]\!]$, $R_i = \tilde{R}_i$, on obtient finalement $Q = \tilde{Q}$, et l'unicité est démontrée.

Lemme A.2.1.5 *On considère les polynômes P et R de $\mathbb{K}[X]$, avec $\deg P \geqslant 1$. Alors, il existe une unique suite presque nulle $(S_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}[X]$, telle que :*

$$R = \sum_{n=0}^{+\infty} S_n P^n \tag{A.5}$$

(Autrement dit : $R = S_0 + S_1 P + \cdots + S_k P^k$) et

$$(\forall n \in \mathbb{N}) \quad \deg S_n < \deg P \tag{A.6}$$

Démonstration A.2.1.5 Montrons l'existence de la suite, par récurrence sur le degré de R. Pour $\deg R < \deg P$, alors $S_0 = R$ et $S_n = 0$ pour $n > 0$, convient. Supposons l'existence de la suite démontrée pour tout polynôme de degré inférieur ou égal à r et supposons $\deg R = r + 1$. Si $r + 1 < \deg P$, le problème est déjà réglé. Supposons $r+1 \geqslant \deg P$. La division euclidienne de R par P donne alors $R = S+PT$, avec $\deg S < \deg P$. Soit $T = 0$, mais alors $\deg R < \deg P$; soit $T \neq 0$ et alors, comme $\deg P \geqslant 1$, on en déduit que $\deg R = \deg PT = \deg P + \deg T > \deg T$, donc $\deg T \leqslant r$. Il ne reste plus dans ce cas qu'a appliquer l'hypothèse de récurrence à T. Il existe donc $(T_n)_{n\in\mathbb{N}}$ presque nulle telle que $T = \sum_{n=0}^{+\infty} T_n P^n$. Mais alors, $R = S + \sum_{n=0}^{+\infty} T_n P^{n+1}$ et la suite définie par $S_0 = S$, $S_n = T_{n-1}$ pour $n > 0$, convient.

Pour obtenir l'unicité, supposons que $(S_n)_{n\in\mathbb{N}}$ et $(\tilde{S}_n)_{n\in\mathbb{N}}$ vérifient A.5 et A.6. Alors $S_0 - \tilde{S}_0 = \sum_{n=1}^{+\infty}(\tilde{S}_n - S_n)P^n \in (P)$. Mais comme $\deg S_0 - \tilde{S}_0 < \deg P$, on a : $S_0 - \tilde{S}_0 = 0$. On obtient donc en « simplifiant » par P : $\sum_{n=1}^{+\infty} S_n P^{n-1} = \sum_{n=1}^{+\infty} \tilde{S}_n P^{n-1}$. En reprenant les arguments ci-dessus, cette dernière égalité aura pour conséquence $S_1 = \tilde{S}_1$. Etc.

Démonstration A.2.1 D'après le lemme A.2.1.4, il existe Q, $R_1, \cdots, R_m$ dans $\mathbb{K}[X]$, uniquement déterminés, tels que : $\frac{A}{B} = Q + \sum_{i=1}^m \frac{R_i}{{P_i}^{r_i}}$ et pour tout $i \in [\![1, m]\!]$, $\deg R_i < \deg {P_i}^{r_i}$. Appliquons le lemme A.2.1.5 avec $R = R_i$ et $P = P_i$. On obtient $R_i = \sum_{n=0}^{+\infty} S_{i\,n} {P_i}^n$, la suite $(S_{i\,n})_{n\in\mathbb{N}}$ étant déterminée de manière unique. Comme $\deg R_i < \deg {P_i}^{r_i}$, on a $R_i = \sum_{n=0}^{r_i-1} S_{i\,n} {P_i}^n$. D'où $\frac{R_i}{{P_i}^{r_i}} = \sum_{n=0}^{r_i-1} \frac{S_{i\,n}}{{P_i}^{r_i-n}}$, et en posant $j = r_i - n$: $\frac{R_i}{{P_i}^{r_i}} = \sum_{j=1}^{r_i} \frac{S_{i\,r_i-j}}{{P_i}^j}$. D'où le théorème en posant $A_{i\,j} = S_{i\,r_i-j}$.

Faisons fonctionner cette belle théorie sur un exemple simple. Cherchons la décomposition en éléments simples de $\frac{X^3+3X+1}{X^3+X+2}$. Commençons par poser la division :

$$\begin{array}{ccc|c} X^3 & +3X & +1 & X^3+X+2 \\ \hline 0 & 2X & -1 & 1 \end{array}$$

On a donc $\frac{X^3+3X+1}{X^3+X+2} = 1 + \frac{2x-1}{x^3+x+2}$. -1 est une racine évidente de X^3+X+2. Donc, $X+1$ divise X^3+X+2. En effet, $X^3+X+2 = (X+1)(X^2-X+2)$. X^2-X+2 est un polynôme irréductible de $\mathbb{R}[X]$ (Preuve ? Calculer le discriminant). Il existe donc a, b et c dans $\mathbb{R}$ tels que : $\frac{2X-1}{X^3+X+2} = \frac{a}{X+1} + \frac{bX+c}{X^2-X+2}$. Pour terminer les calculs, une méthode classique consiste à multiplier les deux membres de cette dernière égalité par $(X+1)(X^2-X+2)$, puis à développer et réduire, de sorte à obtenir de part et d'autre de l'égalité les formes canoniques de polynômes égaux. Il ne reste plus alors qu'à identifier les coefficients des monômes de même degré. Ce qui donne ici :

$$\begin{gathered} 2X-1 = a(X^2-X+2) + (bX+c)(X+1) \iff \\ 2X-1 = (a+b)X^2 + (-a+b+c)X + 2a + c \iff \\ \left\{ \begin{array}{c} a+b=0 \\ -a+b+c=2 \\ 2a+c=-1 \end{array} \right. \end{gathered}$$

(À terminer).

Bibliographie

[1] Jean-Marie Arnaudiès and Henri Fraysse. *Algèbre*, volume 1 of *Cours de mathématiques*. Dunod, Paris, 1987. ISBN 2-04-016450-2.

[2] Paul Richard Halmos. *Naive set theory*. Springer-Verlag, New York, Heidelberg, Berlin, 1974. ISBN 0-387-90092-6.

[3] Jean-Louis Krivine. *Théorie des ensembles*. Cassini, Paris, 1998. ISBN 2-84225-014-1.

[4] Serge Lang. *Algebra*. Addison-Wesley, 1984. ISBN 0-201-05487-6.

[5] Edmond Ramis, Claude Deschamps, and Jacques Odoux. *Algèbre*, volume 1 of *Cours de mathématiques spéciales*. Masson, Paris, 1993. ISBN 2-225-81501-1.

[5], [1] et [2] sont des ouvrages pour le premier cycle ; alors que [4] et [3] sont plutôt destinés aux étudiants de second et de troisième cycles. On ne peut citer tous les ouvrages dans lesquels les éléments d'algèbre abordés dans ce cours sont traités. Je n'indique donc ici que les ouvrages que j'ai consultés pour préparer mes cours.

Index