ALGÈBRE & GÉOMÉTRIE

algebre-geometrie-MEEF.tex

18/04/2019

Sommaire

Introduction.

Partie I

Notions ensemblistes.

1 Ensembles.

Dans cette section, on rappelle le vocabulaire de base sur les ensembles. La définition de la notion d'ensemble n'est pas abordée ; on se contente de l'intuition qu'on en a.

1.1 Rappels de vocabulaire.

Comme on l'a dit précédemment, la notion d'ensemble ne sera pas définie de façon rigoureuse dans ce cours et on se contentera de la représentation intuitive qu'on en a. Un ensemble est défini par la donnée de ses éléments. Rappelons qu'un ensemble qui n'a qu'un élément est appelé un *singleton*. Enfin, l'*ensemble vide* est l'ensemble qui n'a aucun élément ; il est noté $\emptyset$.

Les ensembles de référence que l'on supposera connus sont $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Dans un premier temps, on se contentera de leur définition naïve telle qu'elle a été introduite au Lycée. Néanmoins, on reviendra en détail sur la construction de certains d'entre eux dans des chapitres ultérieurs. Ces ensembles serviront de source d'exemple pour illustrer les différentes notions abordées. On rappelle que $\mathbb{N}$ est l'ensemble des nombres entiers naturels, $\mathbb{Z}$ l'ensemble des nombres entiers relatifs, $\mathbb{Q}$ l'ensemble des nombres rationnels, $\mathbb{R}$ l'ensemble des nombres réels et $\mathbb{C}$ l'ensemble des nombres complexes.

Étant donné un ensemble E, il est souvent utile de distinguer certains éléments parmi tous les éléments. Les éléments que l'on souhaite distinguer forment alors un *sous-ensemble*.

Soient E un ensemble et A un sous-ensemble de E. Soit x un élément de E. Pour exprimer que x est dans A on dit que x *appartient* à A, ce que l'on écrit $x \in A$. Pour exprimer que x n'est pas dans A on dit que x *n'appartient pas* à A, ce que l'on écrit $x \notin A$. Par exemple, si $E = \mathbb{R}$, on a $-1 \notin \mathbb{N}$ et $5 \in \mathbb{N}$.

Étant donné un ensemble E. Si les éléments que l'on souhaite distinguer ne sont pas trop nombreux, on peut expliciter le sous-ensemble qu'ils forment en dressant leur liste exhaustive. Pour ce faire, on utilise une notation avec accolades. Par exemple, on peut considérer le sous-ensemble $\{1, 2, 3, 4\}$ de $\mathbb{N}$. Attention, dans un telle notation, l'ordre dans lequel sont rangés les éléments entre accolades n'a pas d'importance. Ainsi, $\{1, 2, 3, 4\}$ et $\{1, 4, 3, 2\}$ désignent le même sous-ensemble de $\mathbb{N}$. Mais, souvent, les éléments de E que l'on veut distinguer pour former un sous-ensemble sont trop nombreux, voire, en nombre infini. Il est alors impossible d'en dresser la liste exhaustive et, pour les distinguer, on recourt à la notion de *propriété*.

Ainsi, soient E un ensemble et $\mathcal{P}$ une propriété portant sur les éléments de E. Un élément x de E peut satisfaire ou ne pas satisfaire la propriété $\mathcal{P}$. Soit x un élément de E. Si x satisfait la propriété $\mathcal{P}$, on dit que $\mathcal{P}(x)$ est *vraie*, ce que l'on note "$\mathcal{P}(x)$ est vraie" ou, plus simplement, "$\mathcal{P}(x)$". Si x ne satisfait pas la propriété $\mathcal{P}$, on dit que $\mathcal{P}(x)$ est *fausse*.

Il est pratique d'introduire la négation de $\mathcal{P}$. C'est la propriété notée "non-$\mathcal{P}$" et définie par : pour $x \in E$, non-$\mathcal{P}(x)$ est vraie (resp. fausse) si $\mathcal{P}(x)$ est fausse (resp. vraie).

Si $\mathcal{P}$ est une propriété portant sur les éléments de E, on peut définir le sous-ensemble des éléments de E qui vérifient la propriété $\mathcal{P}$. Si l'on note A ce sous-ensemble, on écrit

$$A = \{x \in E \ ; \ \mathcal{P}(x) \text{ est vraie}\} = \{x \in E \ ; \ \mathcal{P}(x)\}.$$

Cette écriture formelle se lit donc "A est l'ensemble des éléments x de E pour lesquels la propriété $\mathcal{P}(x)$ est vraie". Si B est le sous-ensemble des éléments de E qui ne satisfont pas la propriété $\mathcal{P}$,

on a, par exemple :

$$B = \{x \in E \ ; \ \mathcal{P}(x) \text{ est fausse}\} = \{x \in E \ ; \ \text{non-}\mathcal{P}(x)\}.$$

Prenons quelques exemples pour illustrer cette notion. Si $\mathcal{P}$ est la propriété "être inférieur ou égal à 3 et strictement supérieur à -1" portant sur les éléments de $\mathbb{R}$. Alors, le sous-ensemble de $\mathbb{R}$ défini par cette propriété est l'intervalle $]-1,3]$:

$$]-1,3] = \{x \in \mathbb{R} \ ; \ -1 < x \leq 3\}.$$

Si $\mathcal{P}$ est la propriété "être de module 1" portant sur les éléments de $\mathbb{C}$. Alors, le sous-ensemble de $\mathbb{C}$ définit par cette propriété est noté $\mathbb{U}$, et l'on a :

$$\mathbb{U} = \{x \in \mathbb{C} \ ; \ |x| = 1\}.$$

On termine cette section par l'introduction d'un moyen permettant de construire, à partir d'un ensemble donné, un autre ensemble.

Définition 1.1 – *Soit E un ensemble. On appelle puissance de E l'ensemble, noté $\mathcal{P}(E)$, dont les éléments sont les sous-ensembles de E.*

Exemple 1.2 – Considérons l'ensemble E des nombres entiers non nuls, inférieurs ou égaux à 3 : $E = \{1,2,3\}$. Alors,

$$\mathcal{P}(E) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.$$

1.2 Inclusion.

Dans cette sous-section, on considère la situation suivante. On se donne un ensemble E et deux sous-ensembles A et B de E. Le but est alors de comparer A et B.

Pour ce faire, on est amené à introduire la notion d'*inclusion* et d'*égalité* entre sous-ensembles d'un ensemble donné.

Comme on le verra, ces notions, qui portent sur des sous-ensembles, sont étroitement liées aux notions d'*implication* et d'*équivalence* qui, elles, portent sur des propriétés. La compréhension de ce lien est cruciale car c'est sur lui que repose la plupart des démonstrations en mathématiques.

Définition 1.2.1 – *Soient E un ensemble, A et B deux sous-ensembles de E.*
1. On dit que A est inclus dans B, ce que l'on note $A \subseteq B$ (ou parfois $B \supseteq A$), si tout élément de A est élément de B.
2. On dit que A est égal à B, ce que l'on note $A = B$, si $A \subseteq B$ et $B \subseteq A$.

Supposons donnés un ensemble E et deux propriétés $\mathcal{P}$ et $\mathcal{Q}$ portant sur les éléments de E. On commence par quelques rappels de vocabulaire. On dit que $\mathcal{P}$ *implique* $\mathcal{Q}$, ce que l'on note $\mathcal{P} \Longrightarrow \mathcal{Q}$, si tout élément de E qui satisfait $\mathcal{P}$ satisfait aussi $\mathcal{Q}$. On dit que $\mathcal{P}$ *est équivalente à* $\mathcal{Q}$, ce que l'on note $\mathcal{P} \Longleftrightarrow \mathcal{Q}$, si d'une part $\mathcal{P}$ implique $\mathcal{Q}$ et d'autre part $\mathcal{Q}$ implique $\mathcal{P}$.

Soit $x \in E$. Pour dire "si $\mathcal{P}(x)$ est vraie alors $\mathcal{Q}(x)$ est vraie et si $\mathcal{Q}(x)$ est vraie alors $\mathcal{P}(x)$ est vraie" on dit plus simplement "$\mathcal{P}(x)$ est vraie si et seulement si $\mathcal{Q}(x)$ est vraie". Ainsi, dire que $\mathcal{P}$ est équivalente à $\mathcal{Q}$ signifie que, pour tout éléments x de E, x satisfait $\mathcal{P}$ si et seulement

si il satisfait $\mathcal{Q}$.

Définissons alors les sous-ensembles suivants de E :

$$A = \{x \in E \ ; \ \mathcal{P}(x)\} \qquad \text{et} \qquad B = \{x \in E \ ; \ \mathcal{Q}(x)\}.$$

Il découle immédiatement des définissions que la phrase "$A \subseteq B$" est synonyme de la phrase "$\mathcal{P}$ implique $\mathcal{Q}$" et que la phrase "$A = B$" est synonyme de la phrase "$\mathcal{P}$ est équivalente à $\mathcal{Q}$".

1.3 Réunion, intersection, différence.

On commence par définir la réunion, l'intersection et la différence de deux sous-ensembles d'un ensemble donné.

Définition 1.3.1 – *Soient E un ensemble, A et B deux sous-ensembles de E.*
(i) La réunion de A et de B est le sous-ensemble de E composé des éléments qui sont dans A ou dans B. La réunion de A et B est notée $A \cup B$.
(ii) L'intersection de A et de B est le sous-ensemble de E composé des éléments qui sont dans A et dans B. L'intersection de A et B est notée $A \cap B$.
(iii) La différence de A et B est le sous-ensemble de E composé des éléments qui sont dans A et qui ne sont pas dans B. La différence de A et B est notée $A \setminus B$.

Remarque 1.3.2 – Soient E un ensemble, A et B deux sous-ensembles de E.
1. Dans la définition de la réunion de A et de B, il faut bien prendre garde que le *ou* est inclusif (on dit aussi non-exclusif). Cela signifie que l'on accepte, dans $A \cup B$ les éléments qui sont dans A et dans B. Autrement dit, on a :

$$A \cap B \subseteq A \cup B.$$

2. Dans la définition de la réunion et de l'intersection de A et B, l'ordre dans lequel A et B interviennent n'a pas d'importance. Cest-à-dire que $A \cup B = B \cup A$ et $A \cap B = B \cap A$. Il faut bien prendre garde que, en revanche, pour la différence de A et B l'ordre est essentiel. En d'autres termes, $A \setminus B$ et $B \setminus A$ peuvent ne pas être égaux.
3. On a :
(i) $A \cup B = \{x \in E \ ; \ x \in A \text{ ou } x \in B\}$;
(ii) $A \cap B = \{x \in E \ ; \ x \in A \text{ et } x \in B\}$;
(iii) $A \setminus B = \{x \in E \ ; \ x \in A \text{ et } x \notin B\}$.

Exemple 1.3.3 – On se place dans l'ensemble $\mathbb{R}$ et on considère les sous-ensembles $A =]-5, 12]$ et $B = [7, 33]$. Alors, on a $A \cap B = [7, 12]$, $A \cup B =]-5, 33]$, $A \setminus B =]-5, 7[$ et $B \setminus A =]12, 33]$.

Exercice 1.3.4 – Soient E un ensemble et A, B et C des sous-ensembles de E.
1. Montrer que l'on a $A \cup (B \cup C) = (A \cup B) \cup C$. Cet ensemble sera noté $A \cup B \cup C$.
2. Montrer que l'on a $A \cap (B \cap C) = (A \cap B) \cap C$. Cet ensemble sera noté $A \cap B \cap C$.

Définition 1.3.5 – *Soit E un ensemble et A un sous ensemble de E. Le complémentaire de A dans E est l'ensemble des éléments de E qui ne sont pas dans A. Ainsi, le complémentaire de A dans E est la différence $E \setminus A$ de E et de A.*

Remarque 1.3.6 – Soit E un ensemble et A un sous ensemble de E.
1. On a :

$$E \setminus A = \{x \in E \ ; \ x \notin A\}.$$

2. Si A est défini comme l'ensemble des éléments de E qui vérifient une certaine propriété $\mathcal{P}$ portant sur les éléments de E, alors $E \setminus A$ est l'ensemble des éléments de E qui ne vérifie pas $\mathcal{P}$ c'est-à-dire qui vérifient non-$\mathcal{P}$.

Une seconde remarque sur le complémentaire, en lien avec la notion de *démonstration par contrapposée*, s'impose.

Remarque 1.3.7 – Soit E un ensemble.
1. Considérons deux propriétés $\mathcal{P}$ et $\mathcal{Q}$ portant sur les éléments de E. Il est très important de se souvenir du fait suivant. Démontrer que l'on a "$\mathcal{P} \Longrightarrow \mathcal{Q}$" est équivalent à démontrer que l'on a "non-$\mathcal{Q} \Longrightarrow$ non-$\mathcal{P}$". C'est le principe dit de démonstration par contrapposée.
2. Si maintenant on considère les sous-ensembles A et B de E définis par $A = \{x \in E \ ; \ \mathcal{P}(x)\}$ et $B = \{x \in E \ ; \ \mathcal{Q}(x)\}$, le principe de contrapposition se traduit au niveau des ensembles A et B par le fait que $A \subseteq B$ est équivalent à $E \setminus A \supseteq E \setminus B$.

Il est souvent utile de *partager* un ensemble donné en deux parties sans éléments communs. On dit alors qu'on fait une partition de cet ensemble. Voici les définitions rigoureuses permettant de mettre en oeuvre cette idée.

Définition 1.3.8 – *Soient E un ensemble, A et B deux sous-ensembles de E.*
1. On dit que A et B sont disjoints si ils n'ont pas d'éléments en commun.
2. On dit que A et B forment une partition de E si ils sont disjoints et si tout élément de E est dans A ou dans B.

Remarque 1.3.9 – Soient E un ensemble, A et B deux sous-ensembles de E.
1. Dire que A et B sont disjoints signifie que $A \cap B = \emptyset$.
2. Dire que A et B forment une partition de E signifie que $A \cap B = \emptyset$ et $A \cup B = E$.

Exemple 1.3.10 – L'ensemble A des nombres entiers naturels pairs et l'ensemble B des nombres entiers naturels impairs forment une partition de $\mathbb{N}$.

1.4 Produit cartésien.

Dans cette sous-section, on définit un moyen de construire un nouvel ensemble à partir de deux ensembles donnés. Il s'agit de la notion de produit cartésien.

Définition 1.4.1 – *Soient E et F deux ensembles. Le produit cartésien de E et F est l'ensemble dont les éléments sont les couples (e, f) où $e \in E$ et $f \in F$.*

1.5 Relations d'équivalence.

La notion de relation d'équivalence est assez délicate mais très utile dans la suite. On se limite ici au stricte nécessaire pour introduire la notion d'ensemble quotient relatif à une relation d'équivalence.

Définition 1.5.1 – *Soit E un ensemble. Une relation d'équivalence sur E est la donnée d'un sous ensemble $\mathcal{R}$ de $E \times E$ qui satisfait les propriétés suivantes :*
1. $\mathcal{R}$ est réflexif : pour tout $x \in E$, $(x, x) \in \mathcal{R}$;
2. $\mathcal{R}$ est symétrique : pour tous $x, y \in E$, si $(x, y) \in \mathcal{R}$, alors $(y, x) \in \mathcal{R}$;
3. $\mathcal{R}$ est transitif : pour tous $x, y, z \in E$, si $(x, y) \in \mathcal{R}$ et $(y, z) \in \mathcal{R}$, alors $(x, z) \in \mathcal{R}$.

Remarque 1.5.2 – Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. Pour deux éléments x, y de E, il est habituel d'écrire $x\mathcal{R}y$ (qui se lit x est en relation avec y) au lieu de $(x, y) \in \mathcal{R}$. C'est souvent ce que l'on fera dans la suite.

Une relation d'équivalence sur un ensemble E donne lieu à une partition de E, c'est-à-dire qu'elle permet de définir une collection de sous-ensembles deux-à-deux disjoints de E dont E soit la réunion. C'est cet aspect que l'on développe maintenant.

Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence. A tout $x \in E$ on associe l'ensemble $\mathcal{C}_x$, appelé classe d'équivalence de x (pour la relation $\mathcal{R}$), défini par

$$\mathcal{C}_x = \{y \in E \,|\, x\mathcal{R}y\}.$$

Il faut bien prendre garde que si l'on dresse la liste des classes d'équivalences associées à tous les éléments de E, on obtient des redondances. Le résultat suivant permet de clarifier ce point. Il est essentiel pour la suite.

Lemme 1.5.3 – *Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. On a les résultats suivants.*
1. Soit x un élément de E, alors $x \in \mathcal{C}_x$.
2. Soient x et y des éléments de E, alors :
2.1. $x \in \mathcal{C}_y$ si et seulement si $x\mathcal{R}y$;
2.2. $\mathcal{C}_x = \mathcal{C}_y$ si et seulement si $x\mathcal{R}y$;
2.3. $\mathcal{C}_x \cap \mathcal{C}_y \neq \emptyset$ si et seulement si $\mathcal{C}_x = \mathcal{C}_y$.
3. l'ensemble E des classes d'équivalences (deux-à-deux distinctes) de $\mathcal{R}$ est une partition de E.

Démonstration : Certains points sont entièrement démontrés ; pour d'autres, les détails sont laissés au lecteur en exercice.
1. C'est une conséquence immédiate de la réflexivité de $\mathcal{R}$. (Détails en exercices.)
2.1. C'est une conséquence immédiate de la définition de classe d'équivalence. (Détails en exercices.)
2.2. Soient x et y des éléments de E. Supposons que $\mathcal{C}_x = \mathcal{C}_y$. Alors, d'après le point 1, $x \in \mathcal{C}_y$, et donc, d'après 2,1, $x\mathcal{R}y$. Réciproquement, supposons que $x\mathcal{R}y$. On montre d'abord que $\mathcal{C}_x \subseteq \mathcal{C}_y$. Soit $z \in \mathcal{C}_x$. D'après 2.1, $z\mathcal{R}x$. Donc, par transitivité, $z\mathcal{R}y$ ce dont on déduit par 2.1 que $z \in \mathcal{C}_y$. On a montré que $\mathcal{C}_x \subseteq \mathcal{C}_y$. Bien sûr, on démontre de même que $\mathcal{C}_x \supseteq \mathcal{C}_y$. Finalement, on obtient que $\mathcal{C}_x = \mathcal{C}_y$. On a montré l'équivalence des deux assertions de 2.2.
2.3. Soient x et y des éléments de E. Supposons que $\mathcal{C}_x = \mathcal{C}_y$. Alors, $\mathcal{C}_x \cap \mathcal{C}_y = \mathcal{C}_x$. Mais, d'après le point 1, $\mathcal{C}_x$ est non vide. On a prouvé que $\mathcal{C}_x \cap \mathcal{C}_y \neq \emptyset$. Réciproquement, supposons que $\mathcal{C}_x \cap \mathcal{C}_y \neq \emptyset$. Alors, il existe un élément $z \in E$ tel que $z \in \mathcal{C}_x \cap \mathcal{C}_y$. Comme $z \in \mathcal{C}_x$, les points 2.1 et 2.2 assurent que $\mathcal{C}_x = \mathcal{C}_z$. De même, Comme $z \in \mathcal{C}_y$, $\mathcal{C}_y = \mathcal{C}_z$. Finalement $\mathcal{C}_y = \mathcal{C}_x$. Ceci achève la démonstration de ce point.
3. Il s'agit de montrer que tout élément de E est dans une classe d'équivalence et que les classes d'équivalence (deux-à-deux distinctes) ont deux-à-deux une intersection vide. Comme tout élément x de E est dans sa classe (cf. 1), le premier point est clair. Considérons par ailleurs $\mathcal{C}$ et $\mathcal{C}'$ deux classes distinctes pour la relation $\mathcal{R}$. Par définition, il existe x et y dans E tels que $\mathcal{C} = \mathcal{C}_x$ et $\mathcal{C}' = \mathcal{C}_y$. Si l'on suppose que $\mathcal{C} \cap \mathcal{C}' \neq \emptyset$, alors le point 2.3 montre que $\mathcal{C} = \mathcal{C}'$, ce qui est contradictoire. Ainsi $\mathcal{C} \cap \mathcal{C}' = \emptyset$. La démonstration du point 3 est terminée. ∎

On passe maintenant à la notion d'ensemble quotient pour une relation d'équivalence. Pour cela on rappelle que, si E est un ensemble, le *nouvel* ensemble dont les éléments sont *tous les*

sous-ensembles de E est noté $\mathcal{P}(E)$. Avec ce vocabulaire, si $\mathcal{R}$ est une relation d'équivalence sur E, l'ensemble quotient de E par $\mathcal{R}$ est un sous-ensemble de $\mathcal{P}(E)$. On le définit ainsi.

Définition 1.5.4 – *Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. On appelle ensemble quotient de E par $\mathcal{R}$, que l'on note $E/\mathcal{R}$, le sous-ensemble de $\mathcal{P}(E)$ dont les éléments sont les classes d'équivalence pour $\mathcal{R}$. En d'autres termes, $E/\mathcal{R} \subseteq \mathcal{P}(E)$, et un élément $\mathcal{X}$ de $\mathcal{P}(E)$ est dans $E/\mathcal{R}$ s'il existe $x \in E$ tel que $\mathcal{X} = \mathcal{C}_x$.*

La notion de relation d'équivalence est fondamentale dans de nombreuses situations. De notre point de vue, elle servira en particulier à définir les ensembles quotients de $\mathbb{Z}$, dont les éléments sont les *classes de congruence* modulo un entier n de $\mathbb{Z}$. Cette construction sera abordée au chapitre III. Néanmoins, une autre application, probablement plus fondamentale encore, sera mise en évidence dans l'exercice 4.15 du présent chapitre. Pour plus de détails à ce sujet, voir la remarque 2.3.4 de la section 2 à suivre.

On termine par un point de vocabulaire utile.

Définition 1.3 – *Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. Un système complet de représentants des classes d'équivalences de $\mathcal{R}$ est un sous ensemble X de E tel que :*
1. deux éléments distincts de X aient des classes distinctes ;
2. pour tout $y \in E$, il existe $x \in X$ tel que $\mathcal{C}_x = \mathcal{C}_y$.

1.6 Relations d'ordre.

Dans cette courte section, on définit la notion de relation d'ordre. On se contente essentiellement d'en donner la définition et de mettre en évidence le fait qu'il existe des relations d'ordre *totales* et d'autres qui ne le sont pas.

Définition 1.6.1 – *Soit E un ensemble. Une relation d'ordre sur E est la donnée d'un sous-ensemble $\mathcal{R}$ de $E \times E$ qui satisfait les propriétés suivantes :*
1. $\mathcal{R}$ est réflexif : pour tout $x \in E$, $(x, x) \in \mathcal{R}$;
2. $\mathcal{R}$ est anti-symétrique : pour tous $x, y \in E$, si $(x, y) \in \mathcal{R}$ et $(y, x) \in \mathcal{R}$, alors $x = y$;
3. $\mathcal{R}$ est transitif : pour tous $x, y, z \in E$, si $(x, y) \in \mathcal{R}$ et $(y, z) \in \mathcal{R}$, alors $(x, z) \in \mathcal{R}$.

Remarque 1.6.2 – Soient E un ensemble et $\mathcal{R}$ une relation d'ordre sur E. Pour deux éléments x, y de E, il est habituel d'écrire $x \leq y$ (qui se lit x est inférieur à y pour la relation $\mathcal{R}$) au lieu de $(x, y) \in \mathcal{R}$. C'est souvent ce que l'on fera dans la suite. En outre, lorsqu'on utilise cette notation, il est habituel de lui adjoindre la notation $<$, définie de la façon suivante. Si $x, y \in E$, on écrit que $x < y$ (qui se lit x est strictement inférieur à y) si $x \leq y$ et $x \neq y$.

Définition 1.6.3 – *Soient E un ensemble et $\mathcal{R}$ une relation d'ordre sur E. On dit que $\mathcal{R}$ est une relation d'ordre totale sur E si, pour tous x, y dans E, on a $x \leq y$ ou $y \leq x$.*

Exemple 1.6.4 –
1. L'ensemble $\mathbb{N}$ des entiers naturels est muni d'une relation d'ordre total naturelle (voir la section 2 du chapitre II pour les détails).
2. On considère l'ensemble $\mathbb{N} \times \mathbb{N}$ que l'on munit de la relation binaire suivante :

$$\forall\, (m, n),\ (p, q)\ \in \mathbb{N}^2, \quad (m, n) \leq (p, q) \quad \text{si} \quad m \leq p \quad \text{et} \quad n \leq q.$$

Le relation ci-dessus est une relation d'ordre (appelé ordre produit) ; cet ordre n'est pas total.

2 Applications.

Dans cette section, on introduit la notion d'application.

2.1 Définition.

La définition intuitive de la notion d'application d'un ensemble X vers un ensemble Y est la suivante : il s'agit d'une machine qui à tout élément de X associe un élément de Y (et un seul). Pour passer de l'intuition à une définition rigoureuse, il faut faire appel à la notion de graphe.

Définition 2.1.1 – *Soient X et Y deux ensembles. Un graphe dans $X \times Y$ est un sous-ensemble G de $X \times Y$ possédant la propriété suivante : pour tout $x \in X$, il existe un unique $y \in Y$ tel que $(x, y) \in G$.*

Exemple 2.1.2 –
1. Le sous-ensemble $\{(x, y) \in \mathbb{R} \times \mathbb{R} \ ; \ x^2 + y^2 = 1\}$ de $\mathbb{R} \times \mathbb{R}$ n'est pas un graphe.
2. Le sous-ensemble $\{(x, y) \in \mathbb{R} \times \mathbb{R} \ ; \ y = x^2\}$ de $\mathbb{R} \times \mathbb{R}$ est un graphe.
3. Pour tout ensemble X, le sous-ensemble $\{(x, y) \in X \times X \ ; \ x = y\}$ de $X \times X$ (aussi noté $\{(x, x) \ ; \ x \in X\}$) est un graphe.

Définition 2.1.3 – *Soient X et Y deux ensembles. Une application f de X vers Y est un triplet $f = (X, Y, G)$ où G est un graphe de $X \times Y$. On dira que X est l'ensemble de départ de f, que Y est l'ensemble d'arrivé de f et que G est le graphe de f. Pour $x \in X$, l'unique $y \in Y$ tel que $(x, y) \in G$ est noté $f(x)$ et est appelé l'image de x par f.*

Remarque 2.1.4 – Dans la pratique, une application $f = (X, Y, G)$ de l'ensemble X vers l'ensemble Y sera plutôt notée $f : X \longrightarrow Y$ ou encore

$$\begin{array}{rccc} f & : & X & \longrightarrow & Y \\ & & x & \mapsto & f(x) \end{array} .$$

Le graphe qui définit f n'est alors plus explicite dans l'expression de f mais on le retrouve par $G = \{(x, f(x)) \ ; \ x \in X\}$. Lorsque qu'on mentionnera une application par la notation $f : X \longrightarrow Y$, on notera souvent son graphe G_f.

Remarque 2.1.5 –
1. Il faut bien noter qu'une application est la donnée d'un ensemble de départ, d'un ensemble d'arrivée et d'un graphe. Ainsi, dire que deux applications sont égales signifie qu'elles ont même ensemble de départ, même ensemble d'arrivée et même graphe.
2. Par exemple, les applications

$$\begin{array}{rccc} f & : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & & x & \mapsto & \sin(x) \end{array} \quad \text{et} \quad \begin{array}{rccc} g & : &]-\pi, \pi[& \longrightarrow & \mathbb{R} \\ & & x & \mapsto & \sin(x) \end{array}$$

sont distinctes car elles n'ont pas le même ensemble de départ.
3. Soient $f = (X, Y, G)$ une application et A un sous-ensemble de X. Il est clair que $H = \{(x, y) \in X \times Y \ ; \ (x, y) \in G \text{ et } x \in A\}$ est un graphe de $A \times Y$. L'application $g = (A, Y, H)$ est appelée la restriction de f à A et est notée $f_{|A}$. On a donc $f : X \longrightarrow Y$, $g : A \longrightarrow Y$ et, pour tout $x \in A$, $g(x) = f(x)$. Par exemple, au point 2 ci-dessus, g est la restriction de f à $]-\pi, \pi[$.

Exemple 2.1.6 – Soit X un ensemble. On a déjà vu que le sous-ensemble $\Delta = \{(x,x) \in X \times X \ ; \ x \in X\}$ de $X \times X$ est un graphe de $X \times X$. On appelle application identique (ou identité) de X l'application, notée id_X, et définie par $\mathrm{id}_X = (X, X, \Delta)$.

Sous certaines conditions de compatibilité, on peut composer les applications. C'est ce que l'on explique maintenant.

Théorème 2.1.7 – *Soient X, Y et Z des ensembles. Soient $f = (X, Y, G_f)$ et $g = (Y, Z, G_g)$ deux applications. Le sous-ensemble*

$$G = \{(x,z) \in X \times Z \ ; \ \textit{il existe } y \in Y \textit{ tel que } (x,y) \in G_f \textit{ et } (y,z) \in G_g\}$$

est un graphe de $X \times Z$.

Démonstration : Soit $x \in X$. Puisque G_f est un graphe, il existe $y \in Y$ tel que $(x,y) \in G_f$. Comme G_g est un graphe, il existe alors $z \in Z$ tel que $(y,z) \in G_g$. Par définition de G, on a donc $(x,z) \in G$.

Soient $x \in X$ et z et z' des éléments de Z tels que (x,z) et (x,z') soient dans G. Par définition de G, il existe $y, y' \in Y$ tels que $(x,y) \in G_f$, $(y,z) \in G_g$, $(x,y') \in G_f$, $(y',z') \in G_g$. Comme G_f est un graphe, $y = y'$. Comme G_g est un graphe, il s'ensuit que $z = z'$. Ceci montre que G est un graphe. ∎

Définition 2.1.8 – *On reprend les notations du théorème 2.1.7. La composée de f et g est l'application, notée $g \circ f$, et définie par $g \circ f = (X, Z, G)$.*

Remarque 2.1.9 – Soient X, Y, Z des ensembles et $f = (X, Y, G_f)$ et $g = (Y, Z, G_g)$ des applications. Notons $G_{g\circ f}$ le graphe de $g \circ f$. Comme l'assure le théorème 2.1.7, pour tout x dans X, il existe un unique $z \in Z$ tel que $(x,z) \in G_{g\circ f}$. Le premier paragraphe de la démonstration du théorème 2.1.7 assure alors que l'on a $z = g(f(x))$. En conclusion, on a

$$\begin{array}{rccc} g \circ f & : & X & \longrightarrow & Z \\ & & x & \mapsto & g(f(x)) \end{array} .$$

Exercice 2.1.10 – Soient T, X, Y, et Z des ensembles et $f : T \longrightarrow X$, $g : X \longrightarrow Y$ et $h : Y \longrightarrow Z$ des applications. Montrer que $h \circ (g \circ f) = (h \circ g) \circ f$. Cette application est notée $h \circ g \circ f$.

La notion d'*applications réciproques l'une de l'autre* sera utile dans la suite. Elle est définie de la façon suivante.

Définition 2.1.11 – *Soient X, Y des ensembles et $f : X \longrightarrow Y$ et $g : Y \longrightarrow X$ des applications. On dit que f et g sont réciproques l'une de l'autre si $g \circ f = \mathrm{id}_X$ et $f \circ g = \mathrm{id}_Y$.*

Remarque 2.1.12 – Soient X, Y des ensembles et $f : X \longrightarrow Y$ et $g : Y \longrightarrow X$ des applications. Il est clair que les assertions suivantes sont équivalentes :
1. f et g sont réciproques l'une de l'autre ;
2. pour tout $x \in X$, $g \circ f(x) = x$, et pour tout $y \in Y$, $f \circ g(y) = y$.

Soient X, Y des ensembles et $f : X \longrightarrow Y$ une application. La question de savoir si il existe une application $g : Y \longrightarrow X$ telle que f et g soient réciproques l'une de l'autre est souvent cruciale. On verra plus loin que c'est la notion de *bijectivité* qui permet de traiter cette question. Cependant, on peut dès à présent montrer qu'il existe au plus une telle application. C'est l'objet du prochain énoncé.

Proposition 2.1.13 – *Soient X, Y des ensembles et $f : X \longrightarrow Y$ une application. Si $g : Y \longrightarrow X$ et $g' : Y \longrightarrow X$ sont des applications telles que f et g d'une part et f et g' d'autre part soient réciproques l'une de l'autre, alors $g = g'$.*

Démonstration : Soit $y \in Y$. Puisque f et g sont réciproques l'une de l'autre, on a $f \circ g = \mathrm{id}_Y$. Ainsi, $f \circ g(y) = y$. Mais, on a aussi $g \circ f = g' \circ f = \mathrm{id}_X$. Il vient donc

$$g(y) = g(f \circ g(y)) = (g \circ f \circ g)(y) = g \circ f(g(y)) = g' \circ f(g(y)) = g'(f \circ g(y)) = g'(y).$$

On a donc montré que, pour tout $y \in Y$, $g(y) = g'(y)$, ce qui prouve que $g = g'$. ∎

On termine sette section par la définition d'application croissante d'un ensemble ordonné vers un autre.

Définition 2.1 – *Soient E, F des ensembles ordonnés et $f : E \longrightarrow F$ une application de E vers F. On note $\leq$ l'ordre de E et $\preceq$ l'ordre de F.*
1. On dit que f est croissante (resp. décroissante) si, pour tous $x, y \in E$, si $x \leq y$, alors $f(x) \preceq f(y)$ (resp. $f(x) \succeq f(y)$).
2. On dit que f est strictement croissante (resp. strictemenrt décroissante) si, pour tous $x, y \in E$, si $x < y$, alors $f(x) \prec f(y)$ (resp. $f(x) \succ f(y)$).

2.2 Injections, surjections, bijections.

Définition 2.2.1 – *Soient X, Y des ensembles et $f : X \longrightarrow Y$ une application de X vers Y. Soit $y \in Y$. On appelle antécédent de y par f tout élément $x \in X$ tel que $y = f(x)$.*

Définition 2.2.2 – *Soient X, Y des ensembles et $f : X \longrightarrow Y$ une application de X vers Y.*
1. On dit que $f : X \longrightarrow Y$ est injective si tout élément de l'ensemble d'arrivée Y de f admet au plus un antécédent.
2. On dit que $f : X \longrightarrow Y$ est surjective si tout élément de l'ensemble d'arrivée Y de f admet au moins un antécédent.
3. On dit que $f : X \longrightarrow Y$ est bijective si tout élément de l'ensemble d'arrivée Y de f admet un antécédent et un seul.

Exercice 2.2.3 –
1. Montrer que l'application $f : \mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto x^2$ n'est ni injective ni surjective.
2. Montrer que l'application $g : \mathbb{R} \longrightarrow \mathbb{R}^+$, $x \mapsto x^2$ est surjective.
3. Montrer que l'application $h : \mathbb{R}^+ \longrightarrow \mathbb{R}$, $x \mapsto x^2$ est injective.

Exercice 2.2.4 – Montrer que toute restriction d'une application injective est injective. Montrer qu'une restriction d'une application surjective n'est pas nécessairement surjective.

La proposition suivante explicite la procédure la plus courante pour démontrer qu'une application est injective.

Proposition 2.2.5 – *Soient X, Y des ensembles et $f : X \longrightarrow Y$ une application de X vers Y. Les assertions suivantes sont équivalentes :*
1. f est injective ;
2. pour tous $x_1, x_2 \in X$, si $f(x_1) = f(x_2)$, alors $x_1 = x_2$.
3. pour tous $x_1, x_2 \in X$, si $x_1 \neq x_2$, alors $f(x_1) \neq f(x_2)$.

Démonstration : Considérons un couple $(x_1, x_2) \in X \times X$. Les implication "si $f(x_1) = f(x_2)$, alors $x_1 = x_2$" et "si $x_1 \neq x_2$, alors $f(x_1) \neq f(x_2)$" sont les contrapposées l'une de l'autre. Il s'ensuit que les assertions 2 et 3 sont équivalentes. Il est clair que l'assertion 2 est équivalente à l'injectivité de f car elle exprime que si deux éléments de X sont antécédents d'un même élément de Y, alors il doivent être égaux. ∎

Exemple 2.2.6 – On considère l'application

$$\begin{array}{rccc} f & : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & & x & \mapsto & x^3 \end{array}.$$

On va montrer que f est injective. Pour cela on va utiliser deux méthodes différentes. La première repose sur la caractérisation 2 donnée dans la proposition 2.2.5, la seconde repose sur la caractérisation 3 donnée dans cette même proposition.
1. Commençons par une observation. Soient $x_1, x_2 \in \mathbb{R}$. On a

$$f(x_1) - f(x_2) = x_1^3 - x_2^3 = (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2) = (x_1 - x_2)\left(\left(x_1 + \frac{x_2}{2}\right)^2 + \frac{3}{4}x_2^2\right).$$

Enfin, il est clair que le terme $\left(x_1 + \frac{x_2}{2}\right)^2 + \frac{3}{4}x_2^2$ est positif ou nul et qu'il est nul si et seulement si x_1 et x_2 sont nuls.
2. Montrons que f est injective à l'aide de la caractérisation 2 de la proposition 2.2.5. Considérons $x_1, x_2 \in \mathbb{R}$. Si l'on suppose que $f(x_1) = f(x_2)$, alors le calcul fait au point 1 ci-dessus assure que $x_1 = x_2$ ou que $\left(x_1 + \frac{x_2}{2}\right)^2 + \frac{3}{4}x_2^2 = 0$. Mais, comme on l'a déjà signalé, si $\left(x_1 + \frac{x_2}{2}\right)^2 + \frac{3}{4}x_2^2 = 0$, on a $x_1 = x_2 = 0$. Dans tous les cas, on a donc $x_1 = x_2$. Avec la caractérisation 2 de la proposition 2.2.5, on en déduit que f est injective.
3. Montrons que f est injective à l'aide de la caractérisation 3 de la proposition 2.2.5. Considérons $x_1, x_2 \in \mathbb{R}$ et supposons que $x_1 \neq x_2$. Comme x_1 et x_2 ne sont pas tous deux nuls, on a $\left(x_1 + \frac{x_2}{2}\right)^2 + \frac{3}{4}x_2^2 > 0$ et $x_1 - x_2 > 0$ ou $x_1 - x_2 < 0$. Compte tenu des propriétés de $\mathbb{R}$, il s'ensuit que $f(x_1) - f(x_2) > 0$ ou $f(x_1) - f(x_2) < 0$. Ainsi, $f(x_1) \neq f(x_2)$. Avec la caractérisation 3 de la proposition 2.2.5, on en déduit que f est injective.

Examinons à présent la notion d'application bijective. La proposition suivante montre qu'une application $f : X \longrightarrow Y$ est bijective si et seulement si il existe une application $g : Y \longrightarrow X$ (nécessairement unique d'après la proposition 2.1.13) telle que f et g soient réciproques l'une de l'autre.

Proposition 2.2.7 – *Soient X, Y des ensembles et $f : X \longrightarrow Y$ une application. Les assertions suivantes sont équivalentes :*
1. f est bijective ;
2. il existe une application $g : Y \longrightarrow X$ telle que f et g soient réciproques l'une de l'autre.

Démonstration : Supposons que f est bijective. Par définition, cela signifie que, pour tout y de Y, il existe un unique élément de X, que l'on note x_y tel que $f(x_y) = y$. On peut donc considérer l'application

$$\begin{array}{rccc} g & : & Y & \longrightarrow & X \\ & & y & \mapsto & x_y \end{array}.$$

Il est immédiat que, pour tout $y \in Y$, $f \circ g(y) = y$. D'autre part, soit $x \in X$. Par définition de g, $g(f(x))$ est l'unique antécédent de $f(x)$ par f, c'est donc x. Ainsi, on a $g(f(x)) = x$. On a donc montré que f et g sont réciproques l'une de l'autre.

Réciproquement, supposons qu'il existe une application $g : Y \longrightarrow X$ telle que f et g soient réciproques l'une de l'autre. Soit y un élément de Y. Puisque $f \circ g = \mathrm{id}_Y$, $g(y)$ est un antécédent de y. D'autre part, si x et x' sont des antécédents de y par f, on a $f(x) = f(x')$ et comme $g \circ f = \mathrm{id}_X$, il s'ensuit que $x = g \circ f(x) = g \circ f(x') = x'$. Ainsi, tout élément de Y admet un antécédent et un seul par f, c'est-à-dire que f est bijective. ∎

Définition 2.2.8 – *Soient X, Y des ensembles et $f : X \longrightarrow Y$ une application bijective. L'unique application $g : Y \longrightarrow X$ telle que f et g soient réciproques l'une de l'autre est notée f^{-1} et est appelée l'application réciproque de f.*

2.3 Image directe et image réciproque.

On termine cette section par un point de vocabulaire utile dans la pratique.

Considérons deux ensembles X et Y et une application $f : X \longrightarrow Y$. Considérons en outre un sous-ensemble A de X et un sous-ensemble B de Y. On pose alors la définition suivante.

Définition 2.3.1 – *On reprend les notations ci-dessus.*
1. L'image directe de A par f est le sous-ensemble de Y, noté $f(A)$, et défini par :

$$f(A) = \{y \in Y \ ; \ \textit{il existe } x \in A \textit{ tel que } y = f(x)\}.$$

2. L'image réciproque de B par f est le sous-ensemble de X, noté $f^{-1}(B)$, et défini par :

$$f^{-1}(B) = \{x \in X \ ; \ f(x) \in B\}.$$

Définition 2.3.2 – *On reprend les notations ci-dessus. L'image directe de X par f est appelé l'image de l'application f.*

Remarque 2.3.3 – On reprend les notations ci-dessus. La définition 2.3.1 peut être reformulée ainsi.
1. L'ensemble $f(A)$ est le sous-ensemble des éléments de Y qui sont image d'au moins un élément de A, ou encore l'ensemble des images par f d'éléments de A.
2. L'ensemble $f^{-1}(B)$ est le sous-ensemble des éléments de X dont l'image par f est dans B, ou encore l'ensemble des antécédents par f d'éléments de B.

Remarque 2.3.4 – On termine cette section par un commentaire très important qui sera développé plus tard (cf. exercice 4.15). Le problème que l'on se pose est le suivant : étant donnés deux ensembles X et Y et une application $f : X \longrightarrow Y$, peut-on associer à f une *nouvelle* application qui soit injective (respect. surjective) et, bien sûr, qui garde en mémoire les informations concernant f.
1. Dans le cas de la surjectivité, c'est très facile. Il suffit de considérer l'application g déduite de f par restriction de l'ensemble d'arrivée de f à $f(X)$:

$$\begin{array}{rccc} g & : & X & \longrightarrow & f(X) \\ & & x & \mapsto & f(x) \end{array}.$$

On a donc

$$\forall\, x \in X, \quad g(x) = f(x).$$

De plus, il est clair que g *conserve toutes les informations sur* f en ce sens que l'on peut reconstruire les images des éléments de X par f à partir de g, comme le montre l'égalité ci-dessus. On peut même préciser ce dernier point ainsi. Considérons l'application

$$\begin{array}{rccc} i_f & : & f(X) & \longrightarrow & Y \\ & & z & \mapsto & z \end{array}$$

alors on a $f = i_f \circ g$ (la vérification est laissée en exercice). Au passage, on a montré le point suivant : *toute application peut se factoriser comme la composée d'une application injective et d'une application surjective.*
2. Le cas de l'injectivité est beaucoup plus délicat. Il requiert la notion de relation d'équivalence et d'ensemble quotient. Il sera traité en détail à l'exercice 4.15.

3 Familles d'éléments d'un ensemble.

Dans la pratique, on est souvent amené a considérer des "collections" d'éléments pris dans un ensemble donné. Pour formaliser correctement cette idée, on recourt à la notion de *famille d'éléments*. Intuitivement, si E est l'ensemble dans lequel on puise les éléments, la détermination d'une famille d'éléments de E requiert un autre ensemble, I, dont les éléments permettront "d'étiqueter" les éléments pris dans E pour composer la famille considérée. En d'autre termes, chaque élément de I sera l'étiquette d'un élément de E et la famille sera la "collection" d'éléments de E ainsi sélectionnés. On est donc amené à la définition suivante.

Définition 3.1 – *Soit E un ensemble. Une famille d'éléments de E indexée par l'ensemble I est la donnée d'une application*

$$\begin{array}{rccc} f & : & I & \longrightarrow & E \\ & & i & \mapsto & a_i \end{array} .$$

La famille correspondante est notée $(a_i)_{i\in I}$.

Remarque 3.2 – On reprend les notations de la définition 3.1.
1. Une famille indexée par I d'éléments de E n'est donc rien d'autre qu'une application de I dans E. Mais, comme on veut plutôt y penser comme à une collection d'éléments de E, on adopte la notation $(a_i)_{i\in I}$ au lieu de $(f(i))_{i\in I}$.
2. Conformément à la définition, il est autorisé, dans une famille, de reprendre plusieurs fois le même élément. Autrement dit, il est possible qu'à deux éléments différents i et j de I ont associe le même élément de E (c-à-d que $a_i = a_j$). Ceci se produit si et seulement si l'application sous-jacente f n'est pas injective.

L'idée que, dans une famille donnée, on puisse répéter plusieurs fois le même élément semble contre-intuitive. Elle est pourtant essentiel. C'est ce qui distingue une famille d'éléments de E d'un sous-ensemble de E. Pour cette raison, on est amené à associer à une famille son *support* qui, intuitivement, est le sous-ensemble (donc en particulier sans répétition) des éléments qui consituent la famille.

Définition 3.3 – *On reprend les notations de la définition 3.1. On appelle sous-ensemble associé à la famille $(a_i)_{i\in I}$ (ou encore support de la famille $(a_i)_{i\in I}$) l'image de f.*

Un des intérêts de la notion de famille est qu'elle permet d'étendre la réunion et l'intersection de sous-ensembles d'un ensemble E au-delà du cas où l'on en considère 2.

Soit E un ensemble. On peut en effet considérer une collection $(A_i)_{i\in I}$ de sous-ensembles de E indexée par I, autrement dit, une famille d'éléments de $\mathcal{P}(E)$ indexé par I.

La réunion et l'intersection de deux sous-ensembles d'un ensemble donnée, telles qu'elles ont été définies ci-avant, se généralisent alors de la façon suivante.

Définition 3.4 – *Soient I un ensemble et $(A_i)_{i\in I}$ une famille indexée par I de sous-ensembles d'un ensemble donné E.*
1. La réunion des sous-ensembles de la famille $(A_i)_{i\in I}$ est le sous-ensemble de E des éléments appartenant à l'un (au moins) des sous-ensembles de la famille $(A_i)_{i\in I}$. La réunion des sous-ensembles de la famille $(A_i)_{i\in I}$ est notée $\bigcup_{i\in I} A_i$.
2. L'intersection des sous-ensembles de la famille $(A_i)_{i\in I}$ est le sous-ensemble de E des éléments appartenant à tous les sous-ensembles de la famille $(A_i)_{i\in I}$. L'intersection des sous-ensembles de la famille $(A_i)_{i\in I}$ est notée $\bigcap_{i\in I} A_i$.

Remarque 3.5 – Soit I un ensemble et $(A_i)_{i\in I}$ une famille indexée par I de sous-ensembles d'un ensemble donné E. On a :
1. $\bigcup_{i\in I} A_i = \{x \in E \ ; \ \text{il existe } i \in I \text{ tel que } x \in A_i\}$;
2. $\bigcap_{i\in I} A_i = \{x \in E \ ; \ \text{pour tout } i \in I,\ x \in A_i\}$.

Exemple 3.6 –
1. Si $E = \mathbb{R}$, $I = \mathbb{N}^*$ et, pour tout $i \in \mathbb{N}^*$, $A_i = [-\frac{1}{i}, \frac{1}{i}]$, alors $\bigcup_{i\in I} A_i = [-1, 1]$ et $\bigcap_{i\in I} A_i = \{0\}$.
2. Si $E = \mathbb{R}^2$, $I = \mathbb{R}$ et, pour tout $i \in \mathbb{R}$, $A_i = \{(x, y) \in \mathbb{R}^2 \ ; \ x^2 + y^2 \leq i^2\}$, alors $\bigcup_{i\in I} A_i = \mathbb{R}^2$ $\bigcap_{i\in I} A_i = \{(0, 0)\}$.

4 *Exercices.*

§A - *Quantificateurs, contre-exemples, etc.*

Exercice 4.1 – Soient E, F des ensembles et $f : E \longrightarrow F$ une application.
1. Exprimer en langage courant puis en langage formel (c'est-à-dire à l'aide des quantificateurs $\forall$ et $\exists$) l'affirmation que f est injective, puis, la négation de cette affirmation.
2. Exprimer en langage courant puis en langage formel l'affirmation que f est surjective, puis, la négation de cette affirmation.
3. Exprimer en langage courant puis en langage formel l'affirmation que f est bijective, puis, la négation de cette affirmation.
4. Proposer un moyen pratique de montrer qu'une application est (resp. n'est pas) injective, surjective, bijective.

Exercice 4.2 – Soit $f : \mathbb{N} \longrightarrow \mathbb{N}$ une application. Exprimer formellement l'affirmation que f est croissante, puis, sa négation.

Exercice 4.3 – On considère l'énoncé suivant : un espace vectoriel E, distinct de $\{0\}$, et dont les seuls sous-espaces vectoriels sont $\{0\}$ et E est de dimension 1. Un étudiant propose le début de raisonnement suivant : *Supposons, par l'absurde, que E n'est pas de dimension* 1. *Comme E*

est distinct de $\{0\}$*, il contient au moins un vecteur non nul* v*. La droite* D *engendrée par* v *est un sous-espace verctoriel distinct de* $\{0\}$ *; on a donc* $D = E$ *et* E *est de dimension* 1*. Contradiction.*

Que pensez-vous de cette solution ? De quel type de raisonnement s'agit-il ? Est-il correct ? Proposez une autre rédaction de cette solution.

§B - *Intersection, réunion, différence, produit cartésien.*

Exercice 4.4 – Soient E un ensemble et A, B, C trois sous-ensembles quelconques de E.
a) Démontrez les égalités suivantes ;
(i) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
(ii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
(iii) $E \setminus (A \cup B) = (E \setminus A) \cap (E \setminus B)$;
(iv) $E \setminus (A \cap B) = (E \setminus A) \cup (E \setminus B)$.
b) Démontrez les égalités suivantes :
(i) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
(ii) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;
(iii) $A \cap (B \setminus C) = (A \cap B) \cap (A \setminus C)$.
c) Démontrez l'équivalence : $(A \subseteq B) \Leftrightarrow (A \cup B = B)$
d) Démontrez l'équivalence : $(B \subseteq C) \Leftrightarrow ((A \cup B \subseteq A \cup C)$ et $(A \cap B \subseteq A \cap C))$.

Exercice 4.5 – Soient A_1 et A_2 deux sous-ensembles d'un ensemble A et B_1 et B_2 deux sous-ensembles d'un ensemble B.
1) Montrez que $(A_1 \times B_1) \cap (A_2 \times B_2) = (A_1 \cap A_2) \times (B_1 \cap B_2)$.
2) Montrez que cela ne marche plus si on remplace $\cap$ par $\cup$.

§C - *Images directes et réciproques.*

Exercice 4.6 – Soit $f : X \to Y$ une application. Montrez que, quels que soient les sous-ensembles A, A_1, A_2 de X et les sous-ensembles B, B_1, B_2 de Y, on a :
(i) $(A_1 \subseteq A_2) \Rightarrow (f(A_1) \subseteq f(A_2))$;
(ii) $(B_1 \subseteq B_2) \Rightarrow (f^{-1}(B_1) \subseteq f^{-1}(B_2))$;
(iii) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$; (iv) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$;
(v) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$;
(vi) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$;
(vii) $A \subseteq f^{-1}(f(A))$;
(viii) $f(f^{-1}(B)) \subseteq B$.

§D - *Injectivité, surjectivité, bijectivité.*

Exercice 4.7 – Pour chacune des applications suivantes dire si elle est injective, surjective, bijective (et si oui donner son application réciproque) :
(i) $\mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto x^2$;
(ii) $\mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto x\sqrt{|x|}$;
(iii) $\mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto x^3$;
(iv) $\mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto \dfrac{x}{1+x^2}$;
(v) $\mathbb{R} \longrightarrow \mathbb{Z}$, $x \mapsto [x]$;
(vi) $\mathbb{R}^2 \longrightarrow \mathbb{R}^2$, $(x, y) \mapsto (2x - 3y, x + y)$;
(vii) $\mathbb{R}^2 \longrightarrow \mathbb{R}^2$, $(x, y) \mapsto (x + y, 3x + 3y)$.

Exercice 4.8 – Montrer que toute application strictement croissante d'un ensemble totalement ordonné vers un autre est injective.

Exercice 4.9 – Soient $f : X \to Y, g : Y \to Z$ des applications.
1. Montrez que :
(i) si f et g sont injectives alors $g \circ f$ est injective ;
(ii) si f et g sont surjectives alors $g \circ f$ est surjective ;
(iii) si $g \circ f$ est injective alors f est injective ;
(iv) si $g \circ f$ est surjective alors g est surjective.
2. Montrer que la bijectivité de $g \circ f$ n'implique ni celle de g ni celle de f.

Exercice 4.10 – Soit $f : X \longrightarrow Y$, une application.
a) Montrer que f est injective si et seulement si il existe une application $g : Y \longrightarrow X$ telle que $g \circ f = \mathrm{id}_X$.
b) Montrer que f est surjective si et seulement si il existe une application $h : Y \longrightarrow X$ telle que $f \circ h = \mathrm{id}_Y$.
c) Montrer que f est bijective si et seulement si il existe une application $k : Y \longrightarrow X$ telle que $k \circ f = \mathrm{id}_X$ et $f \circ k = \mathrm{id}_Y$.

Exercice 4.11 – Soit $f : E \to F$ une application.
1) Démontrez que les assertions suivantes sont équivalentes :
(i) f est injective ;
(ii) Pour tout sous-ensemble X de E, $f^{-1}(f(X)) = X$.
2) Même question avec les deux propositions :
(i) f est surjective ;
(ii) pour tout sous-ensemble Y de F, $f(f^{-1}(Y)) = Y$.

Exercice 4.12 – Soient f, g, h des applications de E dans E.
1) On suppose f injective et $f \circ g = f \circ h$; peut-on en déduire $g = h$?
2) On suppose f surjective et $g \circ f = h \circ f$; peut-on en déduire $g = h$?

Exercice 4.13 – Soit E un ensemble. Montrer que l'ensemble $\mathcal{P}(E)$ des parties de E est équipotent avec l'ensemble des applications de E dans $\{0, 1\}$. (On dit que deux ensembles sont *équipotents* si il existe une bijection de l'un vers l'autre.)

§E - *Relations d'équivalence.*

Exercice 4.14 – Soit E un ensemble. Montrer que la donnée d'une relation d'équivalence sur E est équivalente à celle d'une partition de E.

Exercice 4.15 – **Application injective induite par une application.**
Soient E, F des ensembles et $f : E \longrightarrow F$ une application. On définit sur E une relation binaire $\mathcal{R}$ par : pour $x, y \in E$, $x\mathcal{R}y$ si $f(x) = f(y)$.
1) Montrer que $\mathcal{R}$ est une relation d'équivalence.
2) Soit $E/\mathcal{R}$ l'ensemble des classes d'équivalence pour cette relation.
2.1) Montrer que l'application $s_f : E \longrightarrow E/\mathcal{R}$ qui à $x \in E$ associe sa classe est surjective.
2.2) Montrer que l'application $i_f : E/\mathcal{R} \longrightarrow F$ qui à la classe de $x \in E$ associe $f(x)$ est bien définie et injective.
2.3) Montrer que $f = i_f \circ s_f$. (Cette décomposition s'appelle la décomposition canonique de f.)

Exercice 4.16 – Soient E un ensemble et A une partie de E. On définit sur l'ensemble $\mathcal{P}(E)$ des parties de E une relation binaire $\mathcal{R}$ par : pour $X, Y \in \mathcal{P}(E)$, $X\mathcal{R}Y$ si $X \cap A = Y \cap B$. Montrer que $\mathcal{R}$ est une relation d'équivalence et que l'ensemble des parties de E incluses dans A est un système complet de représentants des classes de cette relation.

§F - *Relations d'ordre.*

Exercice 4.17 – Soit E un ensemble. Montrer que l'inclusion entre sous-ensembles de E permet de définir sur $\mathcal{P}(E)$ une relation d'ordre et que celle-ci n'est totale que si E est vide ou réduit à un singleton.

Partie II

Entiers naturels.

Dans ce chapitre, on aborde l'ensemble des entiers naturels dont l'importance est évidemment fondamentale.

Bien sûr, cet ensemble est bien connu et l'intuition qu'on en a est largement suffisante pour travailler avec. Cependant, si l'on veut construire un édifice mathématique parfaitement cohérent, on ne peut pas se contenter de l'intuition et il faut alors poser la question de la *construction de l'ensemble des entiers naturels*. Les mathématiciens se sont posé cette question et y ont répondu en montrant qu'on pouvait construire de façon rigoureuse un ensemble dont les propriétés sont précisément celles que l'on attend de $\mathbb{N}$ si l'on se fie à l'intuition qu'on en a.

Malheureusement, cette construction ne peut être comprise que si l'on maîtrise parfaitement la théorie des ensembles dont on a déjà dit qu'elle est d'un grand degré de difficulté. La construction de $\mathbb{N}$ dépasse donc largement les objectifs d'un cours de base.

Il s'avère en fait que l'on peut réduire toutes les propriétés de l'ensemble $\mathbb{N}$ ainsi construits a trois d'entre-elles, dites "axiomes de Peano". Dans ce chapitre, on va brièvement indiquer comment l'on peut construire les opérations usuelles de $\mathbb{N}$ ainsi que sa relation d'ordre à partir des axiomes de Peano. On rappelera également les propriétés essentielles de $\mathbb{N}$.

1 L'ensemble des entiers naturels.

Théorème 1.1 – *Il existe un ensemble, noté* $\mathbb{N}$*, un élément* 0 *de* $\mathbb{N}$ *et une application*

$$\begin{array}{rccc} s & : & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & & n & \mapsto & s(n) \end{array}$$

satisfaisant les propriétés suivantes :
(A1) $s(\mathbb{N}) = \mathbb{N} \setminus \{0\}$ *;*
(A2) s *est injective ;*
(A3) si A *est un sous-ensemble de* $\mathbb{N}$ *contenant* 0 *et contenant l'image par* s *de chacun de ses éléments, alors* $A = \mathbb{N}$*.*

Remarque 1.2 – Les assertions (A1), (A2) et (A3) sont appelées *axiomes de Peano*. L'assertion (A3) est appelé l'*axiome de récurrence*. Le rôle de l'application s est de permettre le passage d'un entier naturel à son successeur (au sens intuitif). D'ailleurs, on appelera s l'application *successeur*, d'où le choix de s pour la désigner. Ainsi, on peut dors-et-déjà décider d'utiliser le symbole 1 pour désigner $s(0)$.

L'axiome (A3) ci-dessus a une conséquence immédiate et de la plus grande importance dans la pratique. Elle est énoncée dans le théorème ci-dessous.

Théorème 1.3 – *Soit* $\mathcal{P}$ *une propriété portant sur les éléments de l'ensemble* $\mathbb{N}$*. On suppose que :*
1. $\mathcal{P}(0)$ *est vraie ;*
2. si n *est un élément de* $\mathbb{N}$ *tel que* $\mathcal{P}(n)$ *soit vraie, alors* $\mathcal{P}(s(n))$ *est vraie.*
Alors, $\mathcal{P}(n)$ *est vraie pour tout élément* n *de* $\mathbb{N}$*.*

Démonstration : Notons A le sous-ensemble de $\mathbb{N}$ défini par :

$$A = \{n \in \mathbb{N} \ ; \ \mathcal{P}(n) \text{ est vraie}\}.$$

La condition 1 de l'énoncé exprime que $0 \in A$ et la condition 2 que A contient l'image par s de chacun de ses éléments. L'axiome (A3) ci-dessus affirme donc que $A = \mathbb{N}$, c'est-à-dire que $\mathcal{P}(n)$ est vraie pour tout élément n de $\mathbb{N}$. ∎

Dans la pratique, le théorème 1.3 permet de traiter le problème suivant. On considère une propriété $\mathcal{P}$ portant sur les éléments de l'ensemble $\mathbb{N}$, et l'on souhaite démontrer que $\mathcal{P}(n)$ est vraie pour tout élément n de $\mathbb{N}$. On procède alors en deux étapes. Dans la première étape, dite d'*initialisation*, on démontre que $\mathcal{P}(0)$ est vraie. Dans la seconde, dite d'*itération*, on considère un élément $n \in \mathbb{N}$ quelconque et l'on démontre que, si l'on suppose $\mathcal{P}(n)$ vraie, alors $\mathcal{P}(s(n))$ est vraie. Il reste à appliquer le théorème 1.3 pour conclure que $\mathcal{P}(n)$ est vraie pour tout élément $n \in \mathbb{N}$. On dit alors qu'on a démontrée la propriété $\mathcal{P}$ *par récurrence*.

L'axiome de récurrence ne permet pas seulement de démontrer des propriétés, mais aussi de *construire* des suites. C'est ce qu'illustre le théorème suivant qui va être d'une importance considérable dans la suite.

Théorème 1.4 –
Soient X un ensemble, a un élément de X et $f : X \longrightarrow X$ une application de X vers X. Il existe une unique application $u : \mathbb{N} \longrightarrow X$ de $\mathbb{N}$ vers X satisfaisant les propriétés suivantes :
1. $u(0) = a$;
2. pour tout $n \in \mathbb{N}$, $u(s(n)) = f(u(n))$.

Démonstration : On commence par montrer l'existence de u.

Considérons l'ensemble de tous les sous-ensembles S de $\mathbb{N}\times X$ vérifiant la propriété $\mathcal{P}$ suivante :

$$(0, a) \in S \qquad \text{et} \qquad \forall (n, x) \in \mathbb{N} \times X,\ ((n, x) \in S) \Longrightarrow ((s(n), f(x)) \in S)\,.$$

Notons que $\mathbb{N} \times X$ lui-même vérifie $\mathcal{P}$. On note G le sous-ensemble de $\mathbb{N} \times X$ défini comme intersection de tous les sous-ensembles de $\mathbb{N} \times X$ vérifiant la propriété $\mathcal{P}$. Montrons que G est un graphe. Pour ce faire, considérons alors le sous-ensemble A de $\mathbb{N}$ des éléments n pour lesquels il existe un unique x dans X tels que $(n, x) \in G$:

$$A = \{n \in \mathbb{N}\ ;\ \text{il existe un unique } x \in X \text{ tel que } (n, x) \in G\}.$$

Par définition, montrer que G est un graphe revient à montrer que $A = \mathbb{N}$. C'est ce que l'on fait maintenant, à l'aide de l'axiome de récurrence. On remarque d'abord que G lui-même vérifie la propriété $\mathcal{P}$; c'est facile à établir. En outre, par définition de G, G ne peut pas contenir strictement un sous-ensemble de $\mathbb{N}\times X$ satisfaisant $\mathcal{P}$ et ce fait sera utile dans la suite. Montrons que $0 \in A$. Comme G vérifie $\mathcal{P}$, $(0, a) \in G$. Supposons, en outre, qu'il existe $b \in X$, avec $b \neq a$, tel que $(0, b) \in G$. Il est alors facile de voir que $G \setminus \{(0, b)\}$ vérifir la propriété $\mathcal{P}$ et est strictement contenu dans G. Ceci est une contradiction. Ainsi, $0 \in A$. Soit à présent $n \in \mathbb{N}$. Supposons que $n \in A$. On va montrer que $s(n) \in A$. Par hypothèse, il existe un unique $x \in X$ tel que $(n, x) \in G$. Comme G vérifie $\mathcal{P}$, $(s(n), f(x)) \in G$. Supposons maintenant qu'il existe $y \in X$, $y \neq f(x)$, tel que $(s(n), y) \in G$. Là encore, il est facile de voir que $G \setminus \{(s(n), y)\}$ vérifie la propriété $\mathcal{P}$ et on conclut à une contradiction comme ci-dessus. Ainsi, on a établi que $s(n) \in A$. On a donc montré, compte tenu de l'axiome (A3), que $A = \mathbb{N}$.

Posons alors $u = (\mathbb{N}, X, G)$. On a bien $u : \mathbb{N} \longrightarrow X$ telle que $u(0) = a$ et, pour tout $n \in \mathbb{N}$, $u(s(n)) = f(u(n))$.
Il reste à montrer l'unicité de u. Pour cela, supposns qu'il existe une application $v : \mathbb{N} \longrightarrow X$

telle que $v(0) = a$ et, pour tout $n \in \mathbb{N}$, $v(s(n)) = f(v(n))$. Il est facile de montrer, à l'aide d'une récurrence, que pour tout $n \in \mathbb{N}$, $u(n) = v(n)$. Les détails sont laissés au lecteur. ∎

La première conséquence du Théorème 1.4 est l'unicité de $\mathbb{N}$. On détaille ce point dans la remarque suivante.

Remarque 1.5 – Unicité de $\mathbb{N}$.
1. Il est bien sûr légitime de se demander si il peut exister plusieurs ensembles, très différents les uns des autres, satisfaisant les axiomes de Peano. Si tel était le cas, cela signifierait que ces trois axiomes, à eux seuls, ne suffisent pas à décrire l'ensemble des entiers naturels et, par conséquent, il faudrait ajouter d'autres axiomes pour bien distinguer l'ensemble qu'on cherche à construire.
2. En fait, il s'avère que ces trois axiomes suffisent bien à caractériser $\mathbb{N}$ au sens suivant. Si l'on considère un triplet (E, e, σ) où E est un ensemble, e un élément de E et $\sigma : E \longrightarrow E \setminus \{e\}$, et si l'on suppose que ce triplet vérifie les axiomes de Peano (convenablement retranscrits pour ce triplet), alors il existe une application bijective $\alpha : \mathbb{N} \longrightarrow E$ telle que $\alpha(0) = e$ et telle que $\alpha \circ s = \sigma \circ \alpha$. Cela signifie que E muni de son élément e et de son application σ se comporte exactement comme $\mathbb{N}$ muni de son élément 0 et de son application s.
3. Les détails de la démonstration du point 2 ci-dessus son passés sous silence pour ne pas alourdir l'exposé. Cependant, le lecteur très motivé pourra le démontrer en utilisant le théorème 1.4.

2 Opérations et ordre dans $\mathbb{N}$.

Dans cette section, on va montrer comment, à partir de la présentation axiomatique de $\mathbb{N}$, on peut reconstruire les opérations élémentaires (addition et multiplication), ainsi que la relation d'ordre de $\mathbb{N}$.

En fait, on se limitera à une ?bauche dont on espère qu'elle suggèrera les idées essentielles.

2.1 Additions et multiplication.

On commence par ébaucher la construction de l'addition de deux éléments de $\mathbb{N}$.

Rappelons que l'on note 1 l'image de 0 par l'application *succéseur*.

Fixons un élément p de $\mathbb{N}$. On va définir l'opération "ajouter p" à un élément quelconque de $\mathbb{N}$. Pour cela, appliquons le Théorème 1.4 avec $X = \mathbb{N}$, $f = s$ et $a = p$. On obtient qu'il existe une unique application

$$s_p \ : \ \mathbb{N} \ \longrightarrow \ \mathbb{N}$$

telle que $s_p(0) = p$ et, pour tout $n \in \mathbb{N}$, $s_p(s(n)) = s(s_p(n))$. On remarque aussi que, lorsque $p = 1$, cette application n'est autre que s elle même : c'est-à-dire que $s_1 = s$. Ceci est bien conforme à l'idée intuitive que l'on a des entiers : *prendre le succéseur d'un entier revient à lui ajouter* 1. De même, on note que $s_0 = \mathrm{id}_{\mathbb{N}}$.

Pour deux éléments p et n de $\mathbb{N}$, on pose alors $n + p = s_p(n)$.

Ainsi, pour tout $n, p \in \mathbb{N}$, $n + 0 = n$ et $n + 1 = s(n)$, $0 + p = p$ et $(n + 1) + p = (n + p) + 1$. On a en fait la Proposition suivante.

Proposition 2.1.1 – *L'application*

$$\begin{array}{rccc} + & : & \mathbb{N}\times\mathbb{N} & \longrightarrow & \mathbb{N} \\ & & (n,p) & \mapsto & n+p \end{array}$$

vérifie les propriétés suivantes :
1. *pour tout* $p \in \mathbb{N}$, $0+p=p$ *(*0 *est neutre pour* $+$*) ;*
2. *pour tous* $n,p \in \mathbb{N}$, $n+p=p+n$ *(commutativité) ;*
3. *pour tous* $n,p,q \in \mathbb{N}$, $(n+p)+q=n+(p+q)$ *(associativité).*

Démonstration : Exercice instructif. ∎

Exercice 2.1.2 – Montrer que, pour tous $n,p,q \in \mathbb{N}$, si $n+p=n+q$, alors $p=q$.

Exercice 2.1.3 – Soient p et q des éléments de $\mathbb{N}$. Montrer que si $p+q=0$, alors $p=q=0$. (Indication. On peut démontrer la contrapposée qui s'énonce ainsi : si p ou q est non nul, alors $p+q\neq 0$. Pour démontrer cette dernière assertion, on peut utiliser l'axiome (A1).)

Un procédé semblable (mais un peu plus délicat) permet de construire la multiplication dans $\mathbb{N}$.

STOP RELECTURE

2.2 Relation d'ordre.

Une fois définie l'addition de $\mathbb{N}$, on peut définir une relation d'ordre naturelle sur $\mathbb{N}$.

Définition 2.2.1 – *Soient* $m,n \in \mathbb{N}$. *On dira que* m est inférieur ou égal à n, *ou que* n *est* supérieur ou égal à m *ce que l'on notera* $m \leq n$, *s'il existe un élément* $p \in \mathbb{N}$ *tel que* $n=m+p$.

Il est clair, par définition, que pour tout $n \in \mathbb{N}$, $0 \leq n$.

Proposition 2.2.2 – *Avec les notations ci-dessus, on a :*
1. *pour tout* $n \in \mathbb{N}$, $n \leq n$ *(réflexivité) ;*
2. *pour tous* $m,n \in \mathbb{N}$, *si* $(m \leq n$ *et* $n \leq m)$, *alors* $m=n$ *(symétrie) ;*
3. *pour tous* $m,n,p \in \mathbb{N}$, *si* $(m \leq n$ *et* $n \leq p)$, *alors* $m \leq p$ *(transitivité).*

Démonstration : Exercice. ∎

Deux éléments m,n de $\mathbb{N}$ sont dits *comparables* si $m \leq n$ ou $n \leq m$. La proposition suivante montre que deux éléments de $\mathbb{N}$ sont toujours comparables.

Proposition 2.2.3 – *La relation d'ordre* $\leq$ *est totale. C'est-à-dire que, pour tous* $m,n \in \mathbb{N}$, $m \leq n$ *ou* $n \leq m$.

Idée de démonstration : on note S l'ensemble des éléments de $\mathbb{N}$ qui sont comparables avec tout élément de $\mathbb{N}$. On montre, par récurrence, que $S=\mathbb{N}$. ∎

Soit E un sous-ensemble de $\mathbb{N}$. Un élément a de $\mathbb{N}$ est un *minorant* de E s'il est inférieur ou égal à tout élément de E. Un élément a de $\mathbb{N}$ est un *plus petit élément* de E si a est dans E et est un minorant de E. Un élément a de $\mathbb{N}$ est un *majorant* de E si il est supérieur ou égal à tout élément de E. Un élément a de $\mathbb{N}$ est un *plus grand élément* de E si a est dans E et est un majorant de E.

Exercice 2.2.4 –
1. Toute partie de E admet au plus un plus petit (resp. plus grand) élément.
2. L'ensemble $\mathbb{N}$ admet un plus petit élément mais n'admet pas de plus grand élément.

Proposition 2.2.5 – *Tout sous-ensemble non-vide de $\mathbb{N}$ admet un plus petit élément.*

Démonstration : Soit E un sous-ensemble non-vide de $\mathbb{N}$. On raisonne par l'absurde, c'est-à-dire qu'on suppose que E n'admet pas de plus petit élément et on montre que cela débouche sur une absurdité. Supposons donc que E n'a pas de plus petit élément. Notons S l'ensemble des minorants de E. Bien sûr, $0 \in S$. Comme on suppose que E n'admet pas de plus petit élément, aucun élément de S n'est dans E. Soit $k \in S$. Pour tout $n \in E$, $k \leq n$. Donc, il existe $p \in \mathbb{N}$ tel que $n = k + p$. En outre, on doit avoir $p \neq 0$, sans quoi on aurait un élément dans S et dans E. Mais alors, il existe $q \in \mathbb{N}$ tel que $p = q+1$. D'où $n = (k+1)+q$. Ainsi, $k+1 \in S$. Par récurrence, on a donc montré que $S = \mathbb{N}$. Mais ceci contredit le fait que S et E n'ont pas d'élément commun. ∎

On termine par une notation pratique. Si m, n sont des éléments de $\mathbb{N}$ tels que $m \leq n$, on pose

$$[\![m, n]\!] = \{p \in \mathbb{N} \ ; \ m \leq p \leq n\}.$$

3 Ensembles finis, ensembles infinis.

Définition 3.1 – *Soit E un ensemble.*
1. On dit que E est fini si il est vide ou si il existe $p \in \mathbb{N} \setminus \{0\}$ et une bijection $[\![1, p]\!] \longrightarrow E$.
2. On dit que E est infini si E n'est pas fini.

Ainsi, les ensembles finis de référence sont $\emptyset$ les $[\![1, p]\!]$ où p est un élément non nul de $\mathbb{N}$. On va maintenant préciser le lien entre un ensemble fini et un tel ensemble de référence pour pouvoir définir la notion de *cardinal* d'un ensemble.

Les démonstrations des deux résultats suivants ne sont pas particulièrement difficiles. Cependant, on les admet pour alléger le texte.

Théorème 3.2 – *Soient p, q deux éléments non nuls de $\mathbb{N}$.*
1. Il existe une application injective de $[\![1, p]\!]$ vers $[\![1, q]\!]$ si et seulement si $p \leq q$.
2. Il existe une application surjective de $[\![1, p]\!]$ vers $[\![1, q]\!]$ si et seulement si $p \geq q$.
3. Il existe une application bijective de $[\![1, p]\!]$ vers $[\![1, q]\!]$ si et seulement si $p = q$.

Démonstration : Admis. ∎

Théorème 3.3 – *Soit $p \in \mathbb{N} \setminus \{0\}$ et $f : [\![1, p]\!] \longrightarrow [\![1, p]\!]$ une application. Les assertions suivantes sont équivalentes :*
(i) f est bijective ;
(ii) f est injective ;
(iii) f est surjective.

Démonstration : Admis. ∎

Corollaire 3.4 – *Soit E un ensemble fini et non vide. Il existe un unique élément $p \in \mathbb{N} \setminus \{0\}$ pour lequel il existe un bijection $[\![1, p]\!] \longrightarrow E$.*

Démonstration : L'existence d'un tel élément p est assurée par la définition d'ensemble fini. Supposons maintenant que p, q soient des éléments de $\mathbb{N}\backslash\{0\}$ pour lesquels il existent des bijections $f : [\![1, p]\!] \longrightarrow E$ et $g : [\![1, q]\!] \longrightarrow E$. Alors, l'application $g^{-1} \circ f$ est une bijection de $[\![1, p]\!]$ vers $[\![1, q]\!]$. Le théorème 3.2 assure donc que $p = q$. ∎

Définition 3.5 – *Soit E un ensemble fini et non vide. L'unique élément $p \in \mathbb{N} \setminus \{0\}$ pour lequel il existe un bijection $[\![1, p]\!] \longrightarrow E$ est appelé le cardinal de E. Il est noté* $\mathrm{card}(E)$. *En outre, on pose* $\mathrm{card}(\emptyset) = 0$.

Les théorèmes 3.2 et 3.3 se généralisent facilement aux ensembles fini. Les énoncés correspondants sont les suivants.

Corollaire 3.6 – *Soient E et F deux ensembles finis non-vides de cardinaux respectifs p et q.*
1. Il existe une application injective de E vers F si et seulement si $p \leq q$.
2. Il existe une application surjective de E vers F si et seulement si $p \geq q$.
3. Il existe une application bijective de E vers F si et seulement si $p = q$.

Démonstration : C'est une consequence facile du théorème 3.2. ∎

Corollaire 3.7 – *Soient E un ensemble fini non-vide et $f : E \longrightarrow E$ une application. Les assertions suivantes sont équivalentes :*
(i) f est bijective ;
(ii) f est injective ;
(iii) f est surjective.

Démonstration : C'est une consequence facile du théorème 3.3. ∎

Remarque 3.8 – Le corollaire 3.7 est faux pour les ensembles infinis. Il permet d'ailleurs de démontrer qu'un ensemble est infini. Par exemple, l'application $s : \mathbb{N} \longrightarrow \mathbb{N}$, $n \mapsto n + 1$ est injective (axiome (A2)), mais pas surjective (axiome (A1)). On en déduit que $\mathbb{N}$ est infini.

Théorème 3.9 – *Soit E un ensemble fini et F un sous-ensemble de E. Alors, F est fini et* $\mathrm{card}(F) \leq \mathrm{card}(E)$.

Démonstration : Exercice. ∎

4 Démonstrations par récurrence ; exemples et compléments.

Dans cette section, on revient plus en détail sur les démonstrations par récurrence. On a déjà vu qu'une telle démonstration s'appuie sur le théorème 1.3 qui, quant à lui, repose sur l'axiome (A3).

Pour illustrer la pratique de ce type de démonstration, on traite un exemple en détail.

Exercice 4.1 – Montrer que, pour tout n dans $\mathbb{N}$, $3^{2n} - 2^n$ est divisible par 7. (On rappelle que si a et b sont deux entiers naturels, on dit que a divise b si il existe $k \in \mathbb{N}$ tel que $b = ak$.)

Solution. Soit $\mathcal{P}$ la propriété portant sur les éléments de $\mathbb{N}$ et définie par

$$\mathcal{P}(n) \text{ est vraie lorsque 7 divise } 3^{2n} - 2^n.$$

On va procéder par récurrence.
1. *Initialisation.* Il est clair que $\mathcal{P}(0)$ est vraie puisque $3^{2.0} - 2^0 = 0$ est bien divisible par 7.
2. *Itération.* Soit $n \in \mathbb{N}$. Supposons $\mathcal{P}(n)$ vraie. Cela signifie qu'on suppose que $3^{2n} - 2^n$ est divisible par 7, c'est-à-dire qu'il existe un élément $k \in \mathbb{N}$ tel que $3^{2n} - 2^n = 7k$.

On doit démontrer qu'alors, $\mathcal{P}(n+1)$ est vraie. Or,

$$3^{2(n+1)} - 2^{n+1} = 9.3^{2n} - 2.2^n = (7+2)3^{2n} - 2.2^n = 7.3^{2n} + 2(3^{2n} - .2^n) = 7.3^{2n} + 2.7.k = 7(3^{2n} + 2k).$$

Cette dernière égalité montre que 7 divise $3^{2(n+1)} - 2^{n+1}$, c'est-à-dire que $\mathcal{P}(n+1)$ est vraie.
3. D'après le théorème 1.3, la propriété $\mathcal{P}(n)$ est vraie pour tout élément n de $\mathbb{N}$.

En conclusion, on a montré que, pour tout $n \in \mathbb{N}$, $3^{2n} - 2^n$ est divisible par 7.

Il s'avère que, dans la pratique, il est commode de disposer de quelques variantes du théorème 1.3 plus adaptées aux diverses situations que l'on rencontre. On va donc maintenant énoncer ces variantes.

Première variante. Souvent, une récurrence ne commence pas à 0 mais à 1, 2, *etc.* La première variante du théorème 1.3 prend en charge ce genre de situation.

Théorème 4.2 – *Soient n_0 un élément de $\mathbb{N}$ et $\mathcal{P}$ une propriété portant sur les éléments du sous-ensemble $\{n \in \mathbb{N} \ ; \ n \geq n_0\}$ de $\mathbb{N}$. On suppose que :*
1. $\mathcal{P}(n_0)$ est vraie ;
2. si n est un élément de $\mathbb{N}$ tel que $n \geq n_0$ et $\mathcal{P}(n)$ soit vraie, alors $\mathcal{P}(n+1)$ est vraie.
Alors, $\mathcal{P}(n)$ est vraie pour tout élément $n \geq n_0$ de $\mathbb{N}$.

Démonstration : On considère la propriété $\mathcal{Q}$ définie sur $\mathbb{N}$ par : pour n dans $\mathbb{N}$, $\mathcal{Q}(n)$ est vraie si et seulement si $\mathcal{P}(n_0+n)$ est vraie. Les hypothèses du présent théorème assurent que la propriété $\mathcal{Q}$ satisfait les hypothèses du théorème 1.3. Le théorème 1.3 assure donc que $\mathcal{Q}(n)$ est vraie pour tout $n \in \mathbb{N}$, ce qui revient à dire que $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$. ∎

Deuxième variante. Souvent, on a besoin de supposer que la propriété considérée est vraie, non pas à un certain rang, mais pour tout les entiers inférieurs à un certain rang. La deuxième variante du théorème 1.3 prend en charge ce genre de situation.

Théorème 4.3 – *Soient n_0 un élément de $\mathbb{N}$ et $\mathcal{P}$ une propriété portant sur les éléments du sous-ensemble $\{n \in \mathbb{N} \ ; \ n \geq n_0\}$ de $\mathbb{N}$. On suppose que :*
1. $\mathcal{P}(n_0)$ est vraie ;
2. si n est un élément de $\{n \in \mathbb{N} \ ; \ n \geq n_0\}$ tel que $\mathcal{P}(k)$ soit vraie pour tout élément $k \in \mathbb{N}$ tel que $n_0 \leq k \leq n$, alors $\mathcal{P}(n+1)$ est vraie.
Alors, $\mathcal{P}(n)$ est vraie pour tout élément $n \geq n_0$ de $\mathbb{N}$.

Démonstration : On considère la propriété $\mathcal{Q}$ définie sur $\{n \in \mathbb{N} \ ; \ n \geq n_0\}$ par : pour n dans $\mathbb{N}$, $\mathcal{Q}(n)$ est vraie si et seulement si $\mathcal{P}(k)$ est vraie pour tout élément $k \in \mathbb{N}$ tel que $n_0 \leq k \leq n$. Les hypothèses du présent théorème assurent que la propriété $\mathcal{Q}$ satisfait les hypothèses du théorème 4.2. Le théorème 4.2 assure donc que $\mathcal{Q}(n)$ est vraie pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$, ce qui entraîne bien sûr que $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$. ∎

Exercice 4.4 – Montrer que tout entier $n \geq 2$ est produit de nombres premiers. (On rappelle qu'un élément de $\mathbb{N}$ est dit premier si il est supérieur ou égal à 2 et si ses seuls diviseurs sont 1 et lui-même.

Solution. On considère la propriété $\mathcal{P}$ portant sur les éléments de $\{n \in \mathbb{N} \ ; \ n \geq 2\}$ et définie par

$$\mathcal{P}(n) \text{ est vraie si et seulement si } n \text{ est produit de nombres premiers.}$$

On va procéder par récurrence.
1. *Initialisation.* Il est clair que $\mathcal{P}(2)$ est vraie puisque 2 est premier.
2. *Itération.* Soit $n \in \mathbb{N}$. Supposons $\mathcal{P}(k)$ vraie pour tout entier k tel que $2 \leq k \leq n$. Cela signifie qu'on suppose que tout élément k de $\mathbb{N}$ tel que $2 \leq k \leq n$ est produit de nombres premiers.

On doit démontrer qu'alors, $\mathcal{P}(n+1)$ est vraie. Or, deux cas se présentent. Ou bien $n+1$ est premier et il est bien produit de nombres premiers. Ou bien $n+1$ n'est pas premier. Dans ce second cas, il existe donc deux entiers a, b tels que $2 \leq a, b \leq n$ et $n+1 = ab$. Mais, par hypothèse de récurrence, a et b sont produits de nombres premiers, donc $n+1$ est produit de nombres premiers.
3. D'après le théorème 4.3, la propriété $\mathcal{P}(n)$ est vraie pour tout élément n de $\mathbb{N}$ supérieur ou égal à 2.

En conclusion, on a montré que tout $n \in \mathbb{N}$ supérieur ou égal à 2 est produit de nombres premiers.

Troisième variante. Il arrive qu'une propriété porte sur un sous-ensemble fini de $\mathbb{N}$. La troisième variante du théorème 1.3 prend en charge ce genre de situation. On s'y réfère en parlant de *récurrence finie.*

Théorème 4.5 – *Soient n_0, n_1 des éléments distincts de $\mathbb{N}$ et $\mathcal{P}$ une propriété portant sur les éléments du sous-ensemble $\{n \in \mathbb{N} \ ; \ n_0 \leq n \leq n_1\}$ de $\mathbb{N}$. On suppose que :*
1. $\mathcal{P}(n_0)$ est vraie ;
2. si n est un élément de $\{n \in \mathbb{N} \ ; \ n_0 \leq n \leq n_1 - 1\}$ tel que $\mathcal{P}(n)$ soit vraie, alors $\mathcal{P}(n+1)$ est vraie.
Alors, $\mathcal{P}(n)$ est vraie pour tout élément de $\{n \in \mathbb{N} \ ; \ n_0 \leq n \leq n_1\}$.

Démonstration : On laisse les détails au lecteur. Néanmoins, on lui conseille de considérer la propriété $\mathcal{Q}$ portant sur les éléments de $\{n \in \mathbb{N} \ ; \ n \geq n_0\}$ et définie ainsi. Pour $n_0 \leq n \leq n_1$, $\mathcal{Q}(n)$ est vraie si et seulement si $\mathcal{P}(n)$ est vraie. Pour $n > n_1$, $\mathcal{Q}(n)$ est toujours vraie. ∎

5 *Exercices.*

Exercice 5.1 – Soit $n \in \mathbb{N}^*$. On note p_n le nombre de sous-ensembles d'un ensemble fini à n éléments.
1. Calculez p_1, p_2, p_3, p_4.
2. Quelle formule générale cela suggère-t-il pour p_n ? Votre conjecture est-elle exacte ?

Exercice 5.2 – **Formule du binôme**. Pour tout entier $n \in \mathbb{N}^*$ et tout entier $k \in \{0, \ldots, n\}$ on définit le "coefficient" noté C_n^k par les uns, $\binom{n}{k}$ par les autres :

$$C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)} \quad \text{(avec la convention : } 0! = 1\text{)}.$$

a) Vérifiez que pour $1 \leq k \leq n$ on a : $C_{n+1}^k = C_n^k + C_n^{k-1}$.
b) Montrez que pour tout $n \in \mathbb{N}^*$ et tout $(x, y) \in \mathbb{R}^2$ on a :

$$(x+y)^n = \sum_{k=0}^{n} C_n^k . x^k . y^{n-k}.$$

Exercice 5.3 – Démontrer, par récurrence, le théorème de division euclidienne dans $\mathbb{N}$.

Exercice 5.4 – **Construction de $\mathbb{Z}$.**
On considère l'ensemble $E = \mathbb{N} \times \mathbb{N}$ et la loi de composition interne $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ définie par $(a, b) + (c, d) = (a + c, b + d)$.
1) Vérifier que la l.c.i. $+$ définie sur $\mathbb{N} \times \mathbb{N}$ est associative, commutative et possède un neutre, que l'on précisera.
2) On considère, sur E, la relation binaire $\mathcal{R}$ définie par : pour $(a, b), (c, d) \in E$, $(a, b)\mathcal{R}(c, d)$ si $a + d = c + b$. Montrer que cette relation est une relation d'équivalence, et qu'elle est compatible avec l'addition $+$ de E. On note encore $+$ la l.c.i. induite sur $E/\mathcal{R}$.
3) Montrer que la loi $+$ sur $E/\mathcal{R}$ est associative et commutative, qu'elle admet un neutre et que tout élément admet un symétrique (autrement dit $(E/\mathcal{R}, +)$ est un groupe abélien).
4) Montrer que l'ensemble $\{(n, 0),\ n \in \mathbb{N}\} \cup \{(0, n),\ n \in \mathbb{N}^*\}$ est un système complet de représentants des classes de E pour $\mathcal{R}$. On pose $\mathbb{Z} = E/\mathcal{R}$.
5) Montrer que $\iota : \mathbb{N} \longrightarrow \mathbb{Z}$, $n \mapsto (n, 0)$ est injective et compatible avec l'addition de $\mathbb{N}$ et la l.c.i. définie ci-dessus sur $\mathbb{Z}$.
6) Montrer que l'on peut également définir sur $\mathbb{Z}$ une loi $\times$ de sorte que $(\mathbb{Z}, +, \times)$ soit un anneau commutatif.

Exercice 5.5 – **Construction de $\mathbb{Q}$.**
En vous inspirant de la construction de $\mathbb{Z}$, proposer une construction de $\mathbb{Q}$ comme ensemble quotient de $\mathbb{Z} \times \mathbb{Z}^*$.

Partie III

Entiers relatifs, arithmétique élémentaire.

1 L'anneau $\mathbb{Z}$.

Comme elle est un peu délicate, la définition de $\mathbb{Z}$ ne sera abordée que plus tard en appendice (voir la section 4). On verra que $\mathbb{Z}$ est construit à partir de $\mathbb{N}$. On sera alors en mesure de montrer que l'ensemble $\mathbb{Z}$ ainsi construit vérifie le théorème suivant, que l'on admet pour le moment.

Théorème 1.1 – *L'ensemble $\mathbb{Z}$ des entiers relatifs est un ensemble muni de deux opérations $+$ et $\times$ et d'une application injective $\iota : \mathbb{N} \longrightarrow \mathbb{Z}$ telles que :*
(i) $(\mathbb{Z}, +, \times)$ est un anneau commutatif intègre ;
(ii) ι respecte les opérations $+$ et $\times$ (c-à-d que pour tous $m, n \in \mathbb{N}$, $\iota(m+n) = \iota(m) + \iota(n)$ et $\iota(mn) = \iota(m)\iota(n)$;
(iii) $\iota(0)$ et $\iota(1)$ sont les neutres respectifs des opérations $+$ et $\times$ de $\mathbb{Z}$;
(iv) pour tout élément x de $\mathbb{Z}$, il existe $n \in \mathbb{N}$ tel que $x = \iota(n)$ ou $x = -\iota(n)$.

Les éléments de $\mathbb{Z}$ sont appelés *entiers relatifs* ou *entiers rationnels*. Dans la remarque suivante, on précise et complète quelques points du théorème 1.1.

Remarque 1.2 –
1. Soient m, n dans $\mathbb{N}$. On a :
(i) $\iota(m) = \iota(n) \Longrightarrow m = n$;
(ii) $-\iota(m) = -\iota(n) \Longrightarrow m = n$;
(iii) $-\iota(m) = \iota(n) \Longrightarrow m = n = 0$.
(La démonstration est laissée en exercice. Attention, ces résultats peuvent se démontrer à l'aide de la description de $\mathbb{Z}$ donnée en appendice. Mais, il peuvent aussi se déduire du théorème 1.1.)
2. A proprement parler, $\mathbb{N}$ n'est pas un sous-ensemble de $\mathbb{Z}$. Mais, puisque l'application ι est injective, elle induit une bijection entre $\mathbb{N}$ et l'image $\iota(\mathbb{N})$ de ι. Le sous-ensemble $\{\iota(n)\ ;\ n \in \mathbb{N}\}$ est donc en bijection avec $\mathbb{N}$. Dans la pratique, on identifie $\mathbb{N}$ et cet ensemble. Cela signifie que l'on confond un entier naturel n avec son image $\iota(n)$ par ι. Ainsi, pour tout $n \in \mathbb{N}$, $\iota(n)$ sera noté n et on se permettra l'abus de langage $\mathbb{N} \subseteq \mathbb{Z}$.

Il est important de souligner que cette identification de $\mathbb{N}$ avec un sous-ensemble de $\mathbb{Z}$ est rendue possible par le fait que ι respecte $+$ et $\times$. En effet, si m et n sont des entiers naturels, les additionner dans $\mathbb{N}$ puis "voir" leur somme comme un élément de $\mathbb{Z}$ par identification revient au même que de les "voir" tous deux comme des éléments de $\mathbb{Z}$ et ensuite de les additionner dans $\mathbb{Z}$. C'est ce qu'exprime la première équation du point (ii) du théorème 1.1. La même chose s'applique à la multiplication.
3. Compte tenu de ce qui précède, on obtient la description suivante de $\mathbb{Z}$:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\},$$

cette liste étant sans répétition.
4. Rappelons enfin le point suivant. Dire que $(\mathbb{Z}, +, \times)$ est un anneau commutatif intègre signifie qu'il vérifie les propriétés suivantes.
(GC1) pour tous $m, n, p \in \mathbb{Z}$, $(m+n)+p = m+(n+p)$ (associativité de $+$) ;
(GC2) pour tout $m \in \mathbb{Z}$, $0 + m = m$ (0 est neutre pour $+$) ;
(GC3) pour tout $m \in \mathbb{Z}$, il existe $n \in \mathbb{Z}$ tel que $m + n = 0$ (tout élément admet un opposé par $+$) ;
(GC4) pour tous $m, n \in \mathbb{Z}$, $m + n = n + m$ ($+$ est commutative) ;
(AC1) pour tous $m, n, p \in \mathbb{Z}$, $(m \times n) \times p = m \times (n \times p)$ (associativité de $\times$) ;
(AC2) pour tout $m \in \mathbb{Z}$, $1 \times m = m$ (1 est neutre pour $\times$) ;

(AC3) pour tous $m, n, p \in \mathbb{Z}$, $p \times (m+n) = p \times m + p \times n$ (distributivité de $\times$ sur $+$) ;
(AC4) pour tous $m, n \in \mathbb{Z}$, $m \times n = n \times m$ ($\times$ est commutative) ;
(INT) $\mathbb{Z}$ n'est pas réduit à un seul élément et, pour tous $m, n \in \mathbb{Z}$, ($mn = 0 \Longrightarrow m = 0$ ou $n = 0$).

Exercice 1.3 –
1. Soient $p, m, n \in \mathbb{Z}$. Si $m+p = n+p$, alors $m = n$. (Indication : utiliser l'existence de l'opposé.)
2. Soient $m, n \in \mathbb{Z}$, on a : $0.m = 0$; $m(-n) = (-m)n = -(mn)$; $(-1)n = -n$.
3. Soient $m, n, p \in \mathbb{Z}$ avec $p \neq 0$. Si $mp = np$, alors $m = n$.
4. Un élément n de $\mathbb{Z}$ est dit inversible si il existe $m \in \mathbb{Z}$ tel que $mn = 1$. Montrer que si $n \in \mathbb{Z}$ est inversible, il existe un unique $m \in \mathbb{Z}$ tel que $mn = 1$. L'élément m est alors appelé l'inverse de n. Montrer que 1 et -1 sont les seuls éléments inversibles de $\mathbb{Z}$.

On définit maintenant une relation d'ordre total sur $\mathbb{Z}$ qui est compatible avec celle définie sur $\mathbb{N}$.

Soient $m, n \in \mathbb{Z}$. On pose

$$m - n = m + (-n).$$

Définition 1.4 – *Soient $m, n \in \mathbb{Z}$. On dira que m* est inférieur ou égal à *n, ou que n est* supérieur ou égal à *m, ce que l'on notera $m \leq n$, si $n - m \in \mathbb{N}$.*

Soient $m, n \in \mathbb{N}$. Compte tenu de l'identification décrite ci-dessus, on peut considérer que $m, n \in \mathbb{Z}$. L'écriture $m \leq n$ a alors deux sens possibles. Soit m, n sont considérés comme éléments de $\mathbb{N}$ et $m \leq n$ signifie "il existe $p \in \mathbb{N}$ tel que $n = m + p$". Soit m, n sont considérés comme des éléments de $\mathbb{Z}$ et $m \leq n$ signifie $n - m \in \mathbb{N}$. Cependant, il est clair que ces deux significations coïncident (exercice facile). Ainsi, la relation $\leq$ définie sur $\mathbb{Z}$ est bien compatible avec celle de $\mathbb{N}$.

La proposition suivante montre que $\leq$ est une relation d'ordre total sur $\mathbb{Z}$.

Proposition 1.5 – *Avec les notations ci-dessus, on a :*
1. pour tout $n \in \mathbb{Z}$, $n \leq n$ (réflexivité) ;
2. pour tous $m, n \in \mathbb{Z}$, si ($m \leq n$ et $n \leq m$), alors $m = n$ (symétrie) ;
3. pour tous $m, n, p \in \mathbb{Z}$, si ($m \leq n$ et $n \leq p$), alors $m \leq p$ (transitivité).
En outre, si $m, n \in \mathbb{Z}$, alors on a $m \leq n$ ou $n \leq m$.

Démonstration : Exercice (assez) facile. ∎

Soit $n \in \mathbb{Z}$. On dira que n est positif si $n \geq 0$ et qu'il est négatif si $n \leq 0$. On vérifie immédiatement que n est positif si et seulement si il est dans $\mathbb{N}$. Enfin, il est clair que le seul entier relatif qui soit positif et négatif est 0.

On termine cette section par la définition de la valeur absolue d'un entier relatif. Soit $n \in \mathbb{Z}$, la *valeur absolue* de n, notée $|n|$, est définie comme suit :

$$\text{pour } n \in \mathbb{Z}, \quad |n| = \begin{cases} n & \text{si } n \in \mathbb{N} \\ -n & \text{si } -n \in \mathbb{N} \end{cases}.$$

Il convient de remarquer que, compte tenu de l'identification de $\mathbb{N}$ à un sous-ensemble de $\mathbb{Z}$, on a ainsi définie une application

$$|.| : \mathbb{Z} \longrightarrow \mathbb{N}.$$

De plus, un élément $n \in \mathbb{Z}$ est positif si et seulement si $|n| = n$ et est négatif si et seulement si $|n| = -n$.

2 Arithmétique élémentaire.

2.1 Divisibilité dans $\mathbb{Z}$.

Définition 2.1.1 – *Soient $m, n \in \mathbb{Z}$. On dit que m divise n (ou que n est un multiple de m), ce que l'on note $m|n$, si il existe $k \in \mathbb{Z}$ tel que $n = km$.*

Exercice 2.1.2 –
1. Montrer que la relation de divisibilité vérifie les assertions suivantes :
(i) pour tout élément $n \in \mathbb{Z}$, $n|n$ (réflexivité) ;
(ii) pour tous $m, n, p \in \mathbb{Z}$, si $m|n$ et $n|p$, alors $m|p$ (transitivité).
2. Montrer que, pour tous $m, n \in \mathbb{Z}$, si $m|n$ et $n|m$, alors $m = n$ ou $m = -n$.

Le théorème suivant est d'une importance capitale. Il établit une propriété fondamentale de $\mathbb{Z}$ appelée *division euclidienne*. Pour le démontrer, on commence par un lemme.

Lemme 2.1.3 – *Soient m et n des entiers relatifs avec $m > 0$. Il existe un entier relatif q et un seul tel que $qm \leq n < (q+1)m$.*

Démonstration : On démontre d'abord l'unicité. Supposons qu'il existe deux entiers q et q' tels que $qm \leq n < (q+1)m$ et $q'm \leq n < (q'+1)m$. Alors, on a $qm \leq n < (q'+1)m$ et $q'm \leq n < (q+1)m$. Donc $q < q'+1$ et $q' < q+1$, autrement dit $q \leq q'$ et $q' \leq q$, c'est-à-dire $q = q'$.
Passons maintenant à l'existence d'un tel entier. On va distinguer trois cas.
– Si $n = 0$, $q = 0$ convient.
– Supposons $n > 0$; l'ensemble $\{p \in \mathbb{N} \,|\, n < pm\}$ est non vide (il contient par exemple $n+1$) et il contient donc un plus petit élément qui est strictement positif car 0 n'est pas dans $\{p \in \mathbb{N} \,|\, n < pm\}$. Ainsi, il existe $q \in \mathbb{N}$ tel que le plus petit élément de $\{p \in \mathbb{N} \,|\, n < pm\}$ soit $q+1$. On a alors $qm \leq n < (q+1)m$.
– Supposons $n < 0$; ce qui précède appliqué à $-n$ assure qu'il existe un entier naturel q' tel que $q'm \leq -n < (q'+1)m$. On a alors $-(q'+1)m < n \leq -q'm$. Si $n = -q'm$, $q = -q'$ convient, sinon $q = -q' - 1$ convient. ∎

Théorème 2.1.4 – **Division euclidienne.** *Soient m et n des entiers relatifs avec $m > 0$. Il existe un couple d'entiers relatifs (q, r) et un seul tel que :*
(i) $n = qm + r$;
(ii) $0 \leq r < m$.
De plus, si $n \in \mathbb{N}$, alors $q \geq 0$.

Démonstration : D'après le lemme 2.1.3, il existe un entier q tel que $qm \leq n < (q+1)m$. Si l'on pose $r = n - qm$, le couple (q, r) convient. De plus, on a $n = qm + r < (q+1)m$. Ceci assure que si $n \geq 0$ on doit avoir $q \geq 0$.

Enfin, si un couple (q, r) satisfait aux conditions (i) et (ii) de l'énoncé, on a en particulier $qm \leq n < (q+1)m$. Un tel q est donc unique d'après 2.1.3. L'unicité de r est une conséquence immédiate de celle de q. ∎

Dans les notations précédentes, on dit que l'on a effectué la division euclidienne de n par m, que q est le quotient et que r est le reste de cette division.

Exercice 2.1.5 – Soient $m, n \in \mathbb{Z}$ avec $m > 0$. Montrer que $m|n$ si et seulement si le reste de la division euclidienne de n par m est nul.

Certains sous-ensembles de $\mathbb{Z}$ sont d'une importance particulière : les *sous-groupes* de $\mathbb{Z}$. On les définit maintenant puis on les détermine de façon explicite.

Définition 2.1.6 – *Soit H un sous-ensemble de $\mathbb{Z}$. On dit que H est un sous-groupe de $\mathbb{Z}$ si :*
(i) $0 \in H$;
(ii) pour tous $m, n \in \mathbb{Z}$, si m et n sont dans H, alors $m + n \in H$;
(iii) pour tout $n \in \mathbb{Z}$, si $n \in H$, alors $-n \in H$.

Pour tout entier $m \in \mathbb{Z}$, on note $m\mathbb{Z}$ le sous-ensemble des éléments qui sont multiples de m. Ainsi,

$$m\mathbb{Z} = \{n \in \mathbb{Z} \ ; \ m|n\}.$$

Exercice 2.1.7 –
1. Soit $n \in \mathbb{Z}$. Montrer que $n\mathbb{Z} = (-n)\mathbb{Z}$.
2. Soient $m, n \in \mathbb{Z}$. Montrer que $n\mathbb{Z} \subseteq m\mathbb{Z}$ si et seulement si m divise n.
3. Montrer que, si $m, n \in \mathbb{N}$ sont distincts, alors $m\mathbb{Z} \neq n\mathbb{Z}$.

Lemme 2.1.8 – *Soit H un sous-groupe de $\mathbb{Z}$ et $m \in \mathbb{Z}$. Si $m \in H$, alors $m\mathbb{Z} \subseteq H$.*

Démonstration : On commence par montrer la propriété suivante : pour tout entier $n \in \mathbb{N}$, $mn \in H$. Pour cela, on procède par récurrence. Comme H est un sous-groupe, il contient 0. La propriété est donc vraie pour $n = 0$. Soit $n \in \mathbb{N}$. Supposons la propriété vraie à l'ordre n, c'est-à-dire que $mn \in H$. Alors, on a $m(n+1) = mn + m$, et comme H est un sous-groupe, l'hypothèse de récurence assure que $m(n+1) \in H$. Ceci achève la démonstration par récurrence. Enfin, si $n \in \mathbb{Z}$ est strictement négatif, alors $nm = -(-n)m$. D'après ce qui précède, $(-n)m \in H$. Mais, H étant un sous-groupe, il contient donc l'opposé nm de $(-n)m$. En conclusion, on a montré que $m\mathbb{Z} \subseteq H$. ∎

Théorème 2.1.9 –
1. Pour tout $n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
2. Si H est un sous-groupe de $\mathbb{Z}$, il existe un unique entier $m \in \mathbb{N}$ tel que $H = m\mathbb{Z}$.

Démonstration : Le point 1 est facile, on le laisse en exercice au lecteur.
Soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, il existe un élément non nul $a \in \mathbb{Z}$. On a donc que a et $-a$ sont dans $\mathbb{Z}$. Il s'ensuit que l'ensemble $H \cap (\mathbb{N} \setminus \{0\})$ est un sous-ensemble non vide de $\mathbb{N}$. A ce titre, il admet un plus petit élément, que l'on note m.

On va montrer que $H = m\mathbb{Z}$. Puisque $m \in H$, le lemme 2.1.8 assure que $m\mathbb{Z} \subseteq H$. Réciproquement, soit $n \in H$. Par division euclidienne de n par m, il existe un couple $(q, r) \in \mathbb{Z}$ tel que $n = qm + r$ et $0 \leq r < m$. Comme $m \in H$, on a $qm \in H$ et donc $r = n - qm \in H$. Mais, par définition de m, cela entraine que $r = 0$. Donc, $n = qm \in m\mathbb{Z}$. Ainsi, on a montré que tout élément de H est dans $m\mathbb{Z}$, c'est-à-dire : $H \subseteq m\mathbb{Z}$.

L'unicité d'un tel entier m découle de l'exercice 2.1.7. ∎

2.2 P.G.C.D. et P.P.C.M.

On commence par introduire la notion de *plus grand commun diviseur* de deux entiers relatifs.

Soient $a, b \in \mathbb{Z}$. L'ensemble des éléments de $\mathbb{Z}$ qui peuvent s'écrire comme somme d'un multiple de a et d'un multiple de b s'exprime par

$$a\mathbb{Z} + b\mathbb{Z} = \{au + bv \ ; \ u, v \in \mathbb{Z}\}.$$

Exercice 2.2.1 – Soient $a, b \in \mathbb{Z}$. Montrer que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

D'après le théorème 2.1.9 et l'exercice 2.2.1, il existe un unique élément δ de $\mathbb{N}$ tel que

$$a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}.$$

On peut donc poser la définition suivante.

Définition 2.2.2 – *Soient $a, b \in \mathbb{Z}$. L'unique élément $\delta \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$ est appelé le plus grand commun diviseur (p.g.c.d. pour simplifier) de $\mathbb{Z}$. Il est noté* $\mathrm{pgcd}(a, b)$.

Remarque 2.2.3 –
1. Il est clair que $\mathrm{pgcd}(0, 0) = 0$. Plus généralement, pour $a \in \mathbb{Z}$, $\mathrm{pgcd}(a, 0) = \mathrm{pgcd}(0, a) = \mathrm{pgcd}(a, a) = |a|$.
2. Pour $a, b \in \mathbb{Z}$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, a)$.
3. Pour $a, b \in \mathbb{Z}$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(-a, b) = \mathrm{pgcd}(a, -b) = \mathrm{pgcd}(-a, -b)$.
4. Si $a, b \in \mathbb{Z}$ ne sont pas tous les deux nuls, $\mathrm{pgcd}(a, b) > 0$.

Le théorème suivant justifie l'appellation de plus grand diviseur commun. Sa démonstration est simple mais très importante car elle met en jeu les propriétés essentielles du p.g.c.d.

Théorème 2.2.4 – Soient $a, b \in \mathbb{Z}$ avec a ou b non nul et $\delta = \mathrm{pgcd}(a, b)$. Alors :
1. il existe u et v dans $\mathbb{Z}$ tels que $\delta = au + bv$;
2. δ divise a et b ;
3. un élément n de $\mathbb{Z}$ divise a et b si et seulement si il divise δ ;
4. si $n \in \mathbb{Z}$ divise a et b, alors $-\delta \leq n \leq \delta$.
5. δ est le plus grand élément (pour $\leq$) de l'ensemble des diviseurs communs à a et b.

Démonstration : Par définition de δ, on a $\delta\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.
1. Il s'ensuit que $\delta \in a\mathbb{Z} + b\mathbb{Z}$, de sorte qu'il existe $u, v \in \mathbb{Z}$ tels que $\delta = au + bv$.
2. Il s'ensuit aussi que $a, b \in \delta\mathbb{Z}$, ce qui signifie que δ divise a et b.
3. Si $n \in \mathbb{Z}$ est diviseur commun à a et b, l'égalité $\delta = au + bv$ montre que n divise δ. Réciproquement, si n divise δ, le point 2 et la transitivité de la relation de division assure qu'il divise a et b.
4. Si $n \in \mathbb{Z}$ divise a et b, alors $|n|$ divise aussi a et b. Ainsi, il existe $k \in \mathbb{N}$ tel que $\delta = k|n|$. Comme a ou b est non nul, on a $\delta \neq 0$, et par suite $k \geq 1$. Il s'ensuit que $\delta \geq |n|$.
5. Ce qui précède montre que l'ensemble des entiers relatifs diviseurs communs de a et b est majoré par δ et contient δ. Le résultat est donc clair. ∎

Remarque 2.2.5 – Les points 1, 2, 3 du théorème 2.2.4 restent vrais lorsque $a = b = 0$ mais 4 et 5 sont faux dans ce cas.

Proposition 2.2.6 – *Soient $a, b, c \in \mathbb{Z}$. Alors* $\mathrm{pgcd}(ca, cb) = |c|\mathrm{pgcd}(a, b)$.

Démonstration : Posons $\delta = \mathrm{pgcd}(a, b)$. On vérifie facilement que $(ca)\mathbb{Z} + (cb)\mathbb{Z} = (|c|\delta)\mathbb{Z}$ (détails laissés au lecteur). Comme $|c|\delta$ est dans $\mathbb{N}$, le résultat s'ensuit. ∎

On présente maintenant une méthode pratique pour calculer le p.g.c.d. de deux entiers. Cette méthode est connue sous le nom d'*algorithme d'Euclide* et elle repose sur un usage systématique de la division euclidienne.

Algorithme d'Euclide. Soient a et b dans $\mathbb{Z}$. On se fixe pour objectif le calcul de $\delta = \text{pgcd}(a, b)$. Si a et b sont nuls, $\delta = 0$. On exclu donc ce cas. Comme on l'a vu plus haut, on peut supposer a et b dans $\mathbb{N}$ et, quite à changer les notations, on peut supposer $b \leq a$.

Commençons par une observation de base.

Remarque 2.2.7 – Soient m, n des éléments de $\mathbb{Z}$, avec $m > 0$. Soient q et r le quotient et le reste de la division euclidienne de n par m, de sorte que l'on a $n = qm + r$ et $0 \leq r < m$. Alors, il est clair que : un entier $p \in \mathbb{Z}$ divise n et m si et seulement si il divise m et r. Il s'ensuit que $\text{pgcd}(n, m) = \text{pgcd}(m, r)$.

Étape 1. On écrit la division euclidienne de a par b.

Il existe $(q_1, r_1) \in \mathbb{Z}^2$ tels que $a = q_1 b + r_1$ et $0 \leq r_1 < b$.

Si $r_1 = 0$, alors b divise a et donc $\delta = b$. Dans ce cas, l'algorithme est terminé. Si $r_1 \neq 0$, alors grâce à la remarque 2.2.7, $\delta = \text{pgcd}(b, r_1)$.

Étape 2. On écrit la division euclidienne de b par r_1.

Il existe $(q_2, r_2) \in \mathbb{Z}^2$ tels que $b = q_2 r_1 + r_2$ et $0 \leq r_2 < r_1$.

Si $r_2 = 0$, alors r_1 divise b et donc $\delta = \text{pgcd}(b, r_1) = r_1$. Dans ce cas, l'algorithme est terminé. Si $r_2 \neq 0$, alors grâce à la remarque 2.2.7, $\delta = \text{pgcd}(r_1, r_2)$.

Étape 3. On écrit la division euclidienne de r_1 par r_2.

Il existe $(q_3, r_3) \in \mathbb{Z}^2$ tels que $r_1 = q_3 r_2 + r_3$ et $0 \leq r_3 < r_2$.

Si $r_3 = 0$, alors r_2 divise r_1 et donc $\delta = \text{pgcd}(r_1, r_2) = r_2$. Dans ce cas, l'algorithme est terminé. Si $r_3 \neq 0$, alors grâce à la remarque 2.2.7, $\delta = \text{pgcd}(r_2, r_3)$.

Étape 4. *etc*

Comme les restes produits par cette succession de divisions euclidiennes forment une suite décroissante d'entiers naturels :

$$b > r_1 > r_2 > r_3 ...,$$

on aboutit nécessairement à un (premier) reste nul et le processus algorithmique s'arrête là. Si le premier reste nul est produit à l'étape ℓ, on peut résumer l'algorithme par :

Étape 1 : $a = q_1 b + r_1, \qquad 0 < r_1 < b, \qquad \delta = \text{pgcd}(b, r_1).$
Étape 2 : $b = q_2 r_1 + r_2, \qquad 0 < r_2 < r_1, \qquad \delta = \text{pgcd}(r_1, r_2).$
Étape 3 : $r_1 = q_3 r_2 + r_3, \qquad 0 < r_3 < r_2, \qquad \delta = \text{pgcd}(r_2, r_3).$
.....
Étape $\ell - 1$: $r_{\ell-3} = q_{\ell-1} r_{\ell-2} + r_{\ell-1}, \qquad 0 \leq r_{\ell-1} < r_{\ell-2}, \qquad \delta = \text{pgcd}(r_{\ell-2}, r_{\ell-1}).$
Étape ℓ : $r_{\ell-2} = q_\ell r_{\ell-1} + r_\ell, \qquad 0 = r_\ell, \qquad \delta = \text{pgcd}(r_{\ell-1}, r_\ell) = r_{\ell-1}.$

Ainsi, le p.g.c.d. de a et b est le dernier reste non nul dans le processus de l'algorithme d'euclide.

En fait, il y a un intérêt supplémentaire à l'algorithme d'Euclide. En "remontant" l'algorithme, on peut obtenir un couple (u, v) explicite d'éléments de $\mathbb{Z}$ tels que $\delta = au + bv$. Les détails de ce procédé sont un peu désagréables à écrire dans le cas général. On se contente donc de l'illustrer sur un exemple. Néanmoins, ce procédé est simple et sera très utile dans la pratique.

Exemple 2.2.8 – On considère les entiers 314 et 51 et on pose $\delta = \text{pgcd}(314, 51)$. On se fixe pour objectif le calcul de δ et d'un couple $(u, v) \in \mathbb{Z}^2$ tel que $\delta = 314u + 51v$.
1) L'algorithme d'Euclide donne :
$314 = 6.51 + 8$,
$51 = 6.8 + 3$,
$8 = 2.3 + 2$,
$3 = 1.2 + 1$,
$2 = 2.1 + 0$.
Donc, $\delta = 1$.
2) En remontant les identitées ci-dessus, il vient que $1 = 3 - 1.2 = 3 - 1.(8 - 2.3) = 3.3 - 8 = 3.(51 - 6.8) - 8 = 3.51 - 19.8 = 3.51 - 19(314 - 6.51) = (-19).314 + 115.51$.

On aborde maintenant la notion d'*entiers premiers entre eux*. Elle débouche sur le très important *Théorème de Gauss*.

Définition 2.2.9 – *Soient $a, b \in \mathbb{Z}$. On dit que a et b sont premiers entre eux si leur p.g.c.d. est* 1.

Exercice 2.2.10 – Soient $a, b \in \mathbb{Z}$. En outre, soient $d \in \mathbb{N}$ un diviseur commun de a et b et k et l des entiers relatifs tels que $a = kd$ et $b = ld$. Montrer que $d = \text{pgcd}(a, b)$ si et seulement si k et l sont premiers entre eux. (Indication : on pourra utiliser la proposition 2.2.6.)

Proposition 2.2.11 – *Soient $a, b \in \mathbb{Z}$. Les assertions suivantes sont équivalentes :*
(i) a et b sont premiers entre eux ;
(ii) les seuls diviseurs communs à a et b sont -1 et 1 ;
(iii) il existe des entiers u et v tels que $1 = au + bv$.

Démonstration : Cela se déduit sans difficulté du théorème 2.2.4. Les détails sont laissés en exercice. ∎

Théorème 2.2.12 (de Gauss) – *Soient a, b, c des éléments de $\mathbb{Z}$. Si a divise bc et si a et b sont premiers entre eux, alors a divise c.*

Démonstration : Comme a et b sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $1 = au + bv$. D'autre part, il existe $k \in \mathbb{Z}$ tel que $bc = ka$. Ainsi, on a $c = acu + bcv = acu + akv = a(cu + kv)$. Donc a divise c. ∎

On est maintenant en mesure de résoudre les équations *diophantiennes*.

Équations diophantiennes. Soient $a, b \in \mathbb{Z}$, non nuls. On se pose le problème de résoudre, dans $\mathbb{Z}$, l'équation (dite "diophantienne") $ax + by = 1$. Autrement dit, on veut déterminer tous les couples $(x, y) \in \mathbb{Z}^2$ tels que $ax + by = 1$.

Observation de départ. D'après la proposition 2.2.11, on sait que cette équation admet des solutions si et seulement si a et b sont premiers entre eux. En outre, si a et b sont premiers entre eux,

l'algorithme d'Euclide (ou plutôt la méthode, vue précédemment sur un exemple, qui consiste à le remonter) permet le calcul explicite d'une solution.

Supposons donc que a et b sont premiers entre eux et supposons calculée une solution (x_0, y_0) de l'équation

$$ax + by = 1 \qquad \text{(E)}$$

A l'aide du théorème de Gauss, on peut déterminer toutes les solutions de (E). Notons $\mathrm{Sol_E}$ l'ensemble des solutions de E. On procède ainsi.

Soit $(x, y) \in \mathbb{Z}^2$.

1-ère Étape. Supposons que (x, y) est solution de (E). Alors, on a :

$$ax + by = 1 = ax_0 + by_0.$$

Il s'ensuit que

$$a(x - x_0) = b(y_0 - y).$$

Mais, a et b sont premiers entre eux. Comme l'équation ci-dessus montre que b divise $a(x - x_0)$, le théorème de Gauss assure que b divise $x - x_0$. Ainsi, il existe $k \in \mathbb{Z}$ tel que $x - x_0 = kb$, c'est-à-dire tel que $x = x_0 + kb$. En remplaçant dans l'équation $a(x - x_0) = b(y_0 - y)$, on en déduit que $y = -ka + y_0$. En conclusion de cette première étape, on a montré que si (x, y) est solution de (E), il existe $k \in \mathbb{Z}$ tel que $(x, y) = (x_0 + kb, y_0 - ka)$. Autrement dit,

$$\mathrm{Sol_E} \subseteq \{(x_0 + kb, y_0 - ka) \ ; \ k \in \mathbb{Z}\}.$$

2-nd Étape. Réciproquement. Considérons un élément k de $\mathbb{Z}$. Alors,

$$a(x_0 + kb) + b(y_0 - ka) = ax_0 + kab + by_0 + kab = ax_0 + by_0 = 1.$$

Ceci montre que

$$\mathrm{Sol_E} \supseteq \{(x_0 + kb, y_0 - ka) \ ; \ k \in \mathbb{Z}\}.$$

En conclusion, on a montré que

$$\mathrm{Sol_E} = \{(x_0 + kb, y_0 - ka) \ ; \ k \in \mathbb{Z}\}.$$

Exercice 2.2.13 – Déterminer tous les couples (x, y) d'entiers relatifs tels que $4x + 15y = 1$.

On termine cette section par une (brève) étude de la notion de *plus petit commun multiple*.

Soient $a, b \in \mathbb{Z}$. L'ensemble des éléments de $\mathbb{Z}$ qui sont multiple de a et multiple de b s'exprime par

$$a\mathbb{Z} \cap b\mathbb{Z}.$$

Exercice 2.2.14 – Soient $a, b \in \mathbb{Z}$. Montrer que $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

D'après le théorème 2.1.9 et l'exercice 2.2.14, il existe un unique élément μ de $\mathbb{N}$ tel que

$$a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}.$$

On peut donc poser la définition suivante.

Définition 2.2.15 – *Soient $a, b \in \mathbb{Z}$. L'unique élément $\mu \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$ est appelé le plus petit commun multiple (p.p.c.m. pour simplifier) de a et b. Il est noté* $\mathrm{ppcm}(a, b)$.

Ainsi, le plus petit commun multiple de a et b est l'unique entier naturel vérifiant la propriété suivante : un entier $n \in \mathbb{Z}$ est multiple commun à a et b si et seulement si il est multiple de μ.

Exercice 2.2.16 – Soient $a, b \in \mathbb{Z}$. Montrer que $\mathrm{ppcm}(a, b) = 0$ si et seulement si a ou b est nul. (Indication : considérer le produit ab.)

Exercice 2.2.17 – Soient $a, b \in \mathbb{Z}$ tous deux non-nuls. On note E le sous-ensemble de $\mathbb{N}$ des entiers naturels non nuls qui sont multiples de a et de b. Montrer que μ est le plus petit élément de cet ensemble.

On se borne à mettre en évidence le lien entre le p.g.c.d. et le p.p.c.m. de deux entiers.

Proposition 2.2.18 – *Soient a et b des entiers tels que $a, b > 0$. On note δ le p.g.c.d. de a et b et on considère les entiers k et l tels que $a = k\delta$ et $b = l\delta$. Alors,* $\mathrm{ppcm}(a, b) = kl\delta$.

Démonstration : Posons $\mu = kl\delta$. On doit montrer que $\mu\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$. Il est clair que μ est multiple de a et de b. Ainsi, $\mu \in a\mathbb{Z} \cap b\mathbb{Z}$ et par suite, $\mu\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$ (voir le lemme 2.1.8). Réciproquement, soit $n \in a\mathbb{Z} \cap b\mathbb{Z}$. Il existe $k', l' \in \mathbb{Z}$ tels que $n = k'a = l'b$. On en déduit que $kk' = ll'$. Ainsi, l divise kk'. Mais, par définition, k et l sont premiers entre eux (voir l'exercice 2.2.10). On est donc en position d'appliquer le théorème de Gauss qui assure que l divise k'. Il existe donc $c \in \mathbb{Z}$ tel que $k' = cl$. Ainsi, $n = k'a = cla = clk\delta = c\mu$ et par suite $n \in \mu\mathbb{Z}$. On a donc montré que $a\mathbb{Z} \cap b\mathbb{Z} \subseteq \mu\mathbb{Z}$. ∎

Corollaire 2.2.19 – *Soient $a, b \in \mathbb{Z}$. On a*

$$\mathrm{pgcd}(a, b)\mathrm{ppcm}(a, b) = |ab|.$$

Démonstration : Le cas ou $a > 0$ et $b > 0$ se déduit immédiatement de la proposition 2.2.18. Le cas où a et b sont non nuls s'en déduit en se ramenant à $|a|$ et $|b|$. Enfin, le cas où a ou b est nul est évident. ∎

2.3 Nombres premiers.

Soit $n \in \mathbb{Z}$, $n > 1$. On sait que n admet au moins deux diviseurs dans $\mathbb{N}$ (et donc au moins 4 dans $\mathbb{Z}$).

Définition 2.3.1 – *On appelle nombre premier tout entier naturel n supérieur ou égal à 2 et dont les seuls diviseurs dans $\mathbb{N}$ sont 1 et n.*

Ainsi, 2, 3, 5, 7, 11 sont premiers. Noter que, par définition, 1 n'est pas premier. Enfin, il est clair que 2 est le seul nombre premier qui soit pair.

On commence par montrer que le sous-ensemble de $\mathbb{N}$ formé des nombres premiers est infini. Pour cela, on a besoin du théorème suivant.

Théorème 2.3.2 – *Tout entier naturel n supérieur ou égal à 2 admet au moins un diviseur premier.*

Démonstration : Si n est premier il admet un diviseur premier, à savoir lui-même. Supposons donc que n n'est pas premier. Par définition, il existe dans $\mathbb{N}$ un diviseur d de n tel que $1 < d < n$. L'ensemble $\{m \in \mathbb{N} \ ; \ 1 < m < n, \ m|n\}$ est donc non vide et par suite, il admet un plus petit élément p. En fait, p est premier. En effet, dans le cas contraire, il existerait un entier naturel q diviseur de p et tel que $1 < q < p$. L'entier q diviserait alors p et donc n, ce qui contredirait la définition de p. ∎

Exercice 2.3.3 – Donner une démonstration alternative du théorème 2.3.2 en procédant par récurrence.

Dans la proposition suivante, on précise un peu le résultat du théorème 2.3.2. Sur le plan théorique cette amélioration n'est pas très intéressante. Mais, sur le plan pratique, elle est très utile pour savoir si un (petit) nombre est premier. Ce fait sera illustré par des exemples.

Proposition 2.3.4 – *Soit n un entier naturel supérieur ou égal à 2. Si n n'est pas premier, il admet un diviseur premier p tel que $p^2 \leq n$.*

Démonstration : Soit p le plus petit élément de l'ensemble $\{m \in \mathbb{N} \ ; \ 1 < m < n, \ m|n\}$. On a vu dans la preuve du théorème 2.3.2 que p est premier. En outre, il existe $k \in \mathbb{N}$ tel que $n = kp$. Mais alors k est un diviseur de n et, comme n n'est pas premier, $k \neq 1$. Ainsi, on a $1 < k < n$ et il s'ensuit que $p \leq k$ et donc que $p^2 \leq kp = n$. ∎

Exemple 2.3.5 – **Crible d'Erathostène.**
On souhaite dresser la liste de tous les nombres premiers inférieurs ou égaux à 99. D'après la proposition 2.3.4, on obtient la liste exhaustive des nombres premiers si l'on exclu de l'ensemble $\{n \in \mathbb{N} \ ; \ 0 \leq n \leq 99\}$ tous les multiples de 2, 3, 5, 7, sauf 2, 3, 5, et 7. Si l'on représente les entiers en question sous la forme du ou d est le chiffre des dizaines et u le chiffre des unités, on obtient la liste des nombres figurant dans le tableau ci-dessous.

$d \backslash u$	0	1	2	3	4	5	6	7	8	9
0	×	×	2	3	×	5	×	7	×	×
1	×	11	×	13	×	×	×	17	×	19
2	×	×	×	23	×	×	×	×	×	29
3	×	31	×	×	×	×	×	37	×	×
4	×	41	×	43	×	×	×	47	×	×
5	×	×	×	53	×	×	×	×	×	59
6	×	61	×	×	×	×	×	67	×	×
7	×	71	×	73	×	×	×	×	×	79
8	×	×	×	83	×	×	×	×	×	89
9	×	×	×	×	×	×	×	97	×	×

Exemple 2.3.6 – On veut répondre à la question suivante : le nombre 337 est-il premier. Une approche frontale consiste à tester tous les entiers compris entre 2 et 336 pour savoir si ils divisent 337 ou pas. C'est un peu long ! D'après la proposition 2.3.4, on peu se limiter aux entiers naturels m tels que $m^2 \leq 337$. Comme $19^2 = 361$, cela signifie que l'on peut se limiter aux entiers m tels que $2 \leq m \leq 19$, ce qui est très accessible. On constate facilement que 337 n'est pas divisible par 2, 3, 5, 7, 11, 13, 17, 19. La proposition 2.3.4 assure alors que 337 est premier.

Théorème 2.3.7 – *L'ensemble des nombres premiers est infini.*

Démonstration : On procède par l'absurde : on suppose que l'ensemble des nombres premiers est fini et on montre que cela conduit à une contradiction.

Supposons donc que l'ensemble P des nombres premiers est fini et notons $p_1, \ldots, p_s$ ses éléments ($s \in \mathbb{N}^*$). Alors, on peut effectuer le produit $N = p_1 \ldots p_s$ de tous les éléments de P. D'après le théorème 2.3.2, $N+1$ admet un diviseur premier p. Mais, p doit être dans P. Il s'ensuit donc que p divise N. Divisant N et $N+1$, p divise 1, ce qui est une contradiction. ∎

Les deux théorèmes suivants sont fondamentaux.

Théorème 2.3.8 – *Soient p un nombre premier et $n \in \mathbb{Z}$. Alors, p et n sont premiers entre eux si et seulement si p ne divise pas n.*

Démonstration : D'après la proposition 2.2.11, p et n sont premiers entre eux si et seulement si les seuls diviseurs communs à p et n sont -1 et 1. Comme p est premier, ses seuls diviseurs sont $-p$, -1, p et 1. Il s'ensuit facilement que l'ensemble des diviseurs communs à p et n est réduit à $\{-1, 1\}$ si et seulement si p ne divise pas n. ∎

Théorème 2.3.9 – *Soit p un nombre premier. Si p divise un produit d'éléments de $\mathbb{Z}$, alors il divise l'un des facteurs.*

Démonstration : On procède par récurrence sur le nombre de facteurs du produit. On considère donc la propriété $\mathcal{P}$ portant sur $\mathbb{N} \setminus \{0\}$ et définie, pour n dans $\mathbb{N} \setminus \{0\}$, par $\mathcal{P}(n)$ est vraie si dans tout produit divisible par p de n facteurs, l'un des facteurs est divisible par p.

Il est clair que $\mathcal{P}(1)$ est vraie. Soit $n \in \mathbb{N} \setminus \{0\}$. Supposons que $\mathcal{P}(n)$ est vraie. On considère un produit $a_1 \ldots a_{n+1}$ d'éléments de $\mathbb{Z}$, divisible par p. On veut montrer que p divise l'un des facteurs de ce produit. Si p divise a_{n+1}, c'est terminé. Sinon, puisque p est premier, le théorème 2.3.8 assure que p et a_{n+1} sont premiers entre eux. Mais alors, le théorème de Gauss s'applique et montre que p divise $a_1 \ldots a_n$. Il reste à appliquer l'hypothèse de récurrence pour en déduire que p divise l'un des a_i. Ainsi, $\mathcal{P}(n+1)$ et vraie. On a montré, par récurrence, que $\mathcal{P}$ est vraie. ∎

Remarque 2.3.10 – Il est clair que l'hypothèse que p est premier est cruciale. Par exemple, 4 divise 10.14 sans diviser ni 10 ni 14.

On en arrive au théorème de décomposition des entiers relatifs en produit de nombres premiers.

Théorème 2.3.11 –
1. Soit $n \in \mathbb{N}$ tel que $n \geq 2$. Il existe des nombres premiers $p_1, \ldots, p_\ell$ deux-à-deux distincts et des entiers strictement positifs $\alpha_1, \ldots, \alpha_\ell$ tels que $n = p_1^{\alpha_1} \ldots p_\ell^{\alpha_\ell}$.
2. Soit $n \in \mathbb{Z}$ tel que $|n| \geq 2$. Il existe $u \in \{-1, 1\}$, des nombres premiers $p_1, \ldots, p_\ell$ deux-à-deux distincts et des entiers strictement positifs $\alpha_1, \ldots, \alpha_\ell$ tels que $n = u p_1^{\alpha_1} \ldots p_\ell^{\alpha_\ell}$. Une telle écriture de n s'appelle une décomposition de n en produit de nombres premiers.
3. Soit $n \in \mathbb{Z}$ tel que $|n| \geq 2$. Si $n = u p_1^{\alpha_1} \ldots p_\ell^{\alpha_\ell}$ et $n = v q_1^{\beta_1} \ldots q_m^{\beta_m}$ sont deux décomposition de n en produit de nombres premiers, alors $u = v$, $\{p_1, \ldots, p_\ell\} = \{q_1, \ldots, q_m\}$ (en particulier $\ell = m$) et, pour tout $1 \leq i \leq \ell$, si $q_i = p_j$, alors $\beta_i = \alpha_j$.

Démonstration : 1. On considère la propriété $\mathcal{P}$ portant sur les éléments de $\mathbb{N} \setminus \{0, 1\}$ et définie, pour $n \in \mathbb{N} \setminus \{0, 1\}$ par : $\mathcal{P}(n)$ est vraie si pour tout $k \in \mathbb{N}$ tel que $2 \leq k \leq n$, k est produit de nombres premiers. On va montrer $\mathcal{P}$ par récurrence. Il est clair que $\mathcal{P}(2)$ est vraie. Soit $n \in \mathbb{N} \setminus \{0, 1\}$. Supposons que $\mathcal{P}(n)$ est vraie. On doit montrer que $\mathcal{P}(n+1)$ est vraie, et pour

cela, il suffit de montrer que $n+1$ est produit de nombres premiers. Si $n+1$ est premier, c'est terminé. Sinon, on peut écrire $n+1 = m_1 m_2$, où m_1, m_2 sont des entiers compris entre 2 et n. Ainsi, par hypothèse de récurrence, m_1 et m_2 sont produits de nombres premiers et par suite $n+1$ l'est aussi. Ceci achève la démonstration de $\mathcal{P}$ par récurrence.
2. Cela se déduit facilement du 1.
3. Étant données deux décompositions de n comme dans l'énoncé, il est clair que $u = v$. On a donc

$$p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell} = q_1^{\beta_1} \dots q_m^{\beta_m}.$$

Cela signifie que p_1 divise le produit $q_1^{\beta_1} \dots q_m^{\beta_m}$. Et, comme p_1 est premier, le théorème 2.3.9 assure qu'il existe $i \in \{1, \dots, m\}$ tel que p_1 divise q_i. Comme q_i est aussi premier, on doit avoir $p_1 = q_i$. En procédant de même avec les autres p_i, on obtient que $\{p_1, \dots, p_\ell\} \subseteq \{q_1, \dots, q_m\}$. En refaisant de même avec les q_i, on obtient l'inclusion dans l'autre sens et par suite l'égalité $\{p_1, \dots, p_\ell\} = \{q_1, \dots, q_m\}$. Comme les p_i et les q_i sont deux-à-deux distincs, il s'ensuit immédiatement que $\ell = m$. Ainsi, quitte à renuméroter les q_i de telle sorte que $p_1 = q_1$, $p_2 = q_2$, *etc*, légalité devient

$$p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell} = p_1^{\beta_1} \dots p_\ell^{\beta_\ell}.$$

Supposons alors que $\alpha_1 \leq \beta_1$. En simplifiant l'identité ci-dessus par $p_1^{\alpha_1}$, on obtient

$$p_2^{\alpha_2} \dots p_\ell^{\alpha_\ell} = p_1^{\beta_1 - \alpha_1} p_2^{\beta_2} \dots p_\ell^{\beta_\ell}.$$

Si $\alpha_1 \neq \beta_1$, on en déduit que p_1 divise $p_2^{\alpha_2} \dots p_\ell^{\alpha_\ell}$. Le théorème 2.3.9 permet d'en déduire que p_1 est égal à l'un des éléments $p_2, \dots, p_\ell$. Ce qui est une contradiction. Ainsi, on doit avoir $\alpha_1 = \beta_1$. On montre de même que, pour $1 \leq i \leq \ell$, $\alpha_i = \beta_i$. ∎

Exemple 2.3.12 – On a : $36 = 2^2.3^2$ et $990 = 2.3^2.5.11$.

On termine par des applications, très utiles dans la pratique, du théorème 2.3.11. Elles permettent de déterminer les diviseurs et multiples d'un entier donné à partir de sa décomposition en produit de nombres premiers ainsi que de calculer le p.g.c.d. et le p.p.c.m. de deux entiers.

Pour pouvoir énoncer ces résultats dans de bonnes conditions, il est utile d'avoir présent à l'esprit le contenu de l'énoncé suivant.

Exercice 2.3.13 – Soient $p_1, \dots, p_\ell$ des nombres premiers deux-à-deux distincts et soient en outre $\alpha_1, \dots, \alpha_\ell, \beta_1, \dots, \beta_\ell$ des entiers naturels. Montrer que si $p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell} = p_1^{\beta_1} \dots p_\ell^{\beta_\ell}$. Alors $\alpha_i = \beta_i$ pour $1 \leq i \leq \ell$.

Proposition 2.3.14 – *Soit $n \in \mathbb{Z}$ tel que $|n| \geq 2$. Soit $n = u p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell}$ la décomposition de n en produit de nombres premiers.*
1. Les diviseurs de n sont les entiers de la forme $p_1^{\beta_1} \dots p_\ell^{\beta_\ell}$ avec $0 \leq \beta_i \leq \alpha_i$ pour tout $1 \leq i \leq \ell$, ainsi que les opposés de ces entiers.
2. Les multiples de n sont les entiers de la forme $p_1^{\beta_1} \dots p_\ell^{\beta_\ell} m$ avec $\beta_i \geq \alpha_i$ pour tout $1 \leq i \leq \ell$, et où m est un entier qui n'est divisible par aucun des nombres $p_1, \dots, p_\ell$, ainsi que les opposés de ces entiers.

Démonstration : Exercice. ∎

Soient m et n deux entiers relatifs dont la valeur absolue est au moins égale à 2. Soient $p_1, \dots, p_\ell$ la liste des nombres premiers deux-à-deux distincts qui divisent m ou n. Alors, il existe des entiers naturels $\alpha_1, \dots, \alpha_\ell, \beta_1, \dots, \beta_\ell$ tels que

$$m = p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell} \quad \text{et} \quad n = p_1^{\beta_1} \dots p_\ell^{\beta_\ell}.$$

Et, d'après l'exercice 2.3.13, ces entiers sont uniquement déterminés.

Proposition 2.3.15 – *Avec les notations ci-dessus, on a :*
1. $\text{pgcd}(m,n) = p_1^{\delta_1} \dots p_\ell^{\delta_\ell}$ *où, pour* $1 \leq i \leq \ell$, $\delta_i = \min\{\alpha_i, \beta_i\}$ *;*
2. $\text{ppcm}(m,n) = p_1^{\mu_1} \dots p_\ell^{\mu_\ell}$ *où, pour* $1 \leq i \leq \ell$, $\mu_i = \max\{\alpha_i, \beta_i\}$.

Démonstration : Exercice. ∎

Exemple 2.3.16 – Considérons les entiers 36 et 990. On a déjà vu que leurs décomposition en produit de facteurs premiers s'écrivent : $36 = 2^2.3^2$ et $990 = 2.3^2.5.11$.
1. On en déduit, par la proposition 2.3.14 que les diviseurs de 990 s'écrivent sous la forme $2^{\beta_1}.3^{\beta_2}.5^{\beta_3}.11^{\beta_4}$, où $0 \leq \beta_1 \leq 1$, $0 \leq \beta_2 \leq 2$, $0 \leq \beta_3 \leq 1$ et $0 \leq \beta_4 \leq 1$. Compte tenu de l'exercice 2.3.13, il s'ensuit qu'il sont au nombre de $2.3.2.2 = 24$.
2. La proposition 2.3.15 montre que $\text{pgcd}(36, 990) = 2.3^2 = 18$ et $\text{ppcm}(36, 990) = 2^2.3^2.5.11 = 1980$.

3 Les anneaux $\mathbb{Z}/n\mathbb{Z}$.

Sauf mention explicite du contraire, dans cette section, n désigne un entier naturel non nul.

3.1 Congruence modulo un entier.

Définition 3.1.1 – *Soient $x, y \in \mathbb{Z}$. On dit que x et y sont congrus modulo n, ce que l'on note*

$$x \equiv y \pmod{n}.$$

si $x - y \in n\mathbb{Z}$.

Remarque 3.1.2 – Ainsi, dire que deux entiers relatifs x, y sont congrus modulo n signifie que leur différence est un multiple de n, c'est-à-dire qu'il existe $k \in \mathbb{Z}$ tel que $x - y = kn$.

La relation de congruence définie ci-dessus vérifie les propriétés suivantes qui ont des conséquences très importantes dans la suite.

Proposition 3.1.3 –
1. Pour tout $x \in \mathbb{Z}$, $x \equiv x \pmod{n}$.
2. Pour tous $x, y \in \mathbb{Z}$, si $x \equiv y \pmod{n}$, alors $y \equiv x \pmod{n}$.
3. Pour tous $x, y, z \in \mathbb{Z}$, si $x \equiv y \pmod{n}$ et $y \equiv z \pmod{n}$, alors $x \equiv z \pmod{n}$.

Démonstration : 1. Il est clair que $x - x = 0$ est un multilple de n. Donc $x \equiv x \pmod{n}$.
2. Si $x \equiv y \pmod{n}$, il existe $k \in \mathbb{Z}$ tel que $x - y = kn$. Il s'ensuit que $y - x = (-k)n$, donc $y \equiv x \pmod{n}$.
3. Si $x \equiv y \pmod{n}$ et $y \equiv z \pmod{n}$, il existe $k, \ell \in \mathbb{Z}$ tels que $x - y = kn$ et $y - z = \ell n$. On a donc $x - z = (x - y) + (y - z) = kn + \ell n = (k + \ell)n$. Donc $x \equiv z \pmod{n}$. ∎

La proposition suivante donne un moyen pratique permettant de dire si deux entiers relatifs sont congrus modulo n. Elle est fondamentale pour la suite.

Proposition 3.1.4 – *Deux entiers relatifs sont congrus modulo n si et seulement si ils ont même reste dans la division euclidienne par n.*

Démonstration : Soient $x, y \in \mathbb{Z}$.
1. Supposons que x et y sont congrus modulo n. Alors, il existe $k \in \mathbb{Z}$ tel que $x - y = kn$. Écrivons la division euclidienne de y par n : il existe $q, r \in \mathbb{Z}$ tels que l'on ait $y = qn + r$ et $0 \leq r < n$. Il s'ensuit que $x = y + kn = (qn + r) + kn = (q + k)n + r$. Cette dernière égalité n'est autre que la division euclidienne de x par n dont le reste est donc bien r.
2. Réciproquement, supposons que x et y ont même reste dans la division euclidienne par n. Alors, il existe $q, q', r \in \mathbb{Z}$ tels que $x = qn + r$ et $y = q'n + r$. Il vient que $x - y = (qn + r) - (q'n + r) = (q - q')n$. Ainsi, x et y sont bien congrus modulo n. ∎

Corollaire 3.1.5 – *Soit $x \in \mathbb{Z}$. Il existe un élément y et un seul de $\{0, \ldots, n-1\}$ tel que x et y soient congrus modulo n. De plus, cet élément est le reste de la division euclidienne de x par n.*

Démonstration : Commençons par remarquer qu'un élément y de $\{0, \ldots, n-1\}$ est son propre reste dans sa division euclidienne par n. En effet, on a $y = 0.n + y$, avec $0 \leq y < n$.

Cette remarque jointe à la proposition 3.1.4 assure donc que x et son reste r dans la division euclidienne par n sont congrus modulo n.

Supposons maintenant que s est un entier de $\{0, \ldots, n-1\}$ tel que x et s soient congrus modulo n. D'après la proposition 3.1.4, x et s ont même reste dans la division euclidienne par n. Mais, toujours d'après la remarque du début de cette démonstration, cela assure que s est le reste de x dans sa division euclidienne par n. ∎

3.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$.

Définition 3.2.1 – *Soit $x \in \mathbb{Z}$. On appelle classe d'équivalence de x modulo n le sous-ensemble de tous les entiers y de $\mathbb{Z}$ tels que x et y soient congrus modulo n. La classe d'équivalence de x modulo n sera notée $\overline{x}$.*

Attention, la notation $\overline{x}$ pour la classe d'équivalence de x présente un sérieux inconvenient : elle ne fait pas mention de n. Ainsi, si l'on est dans une situation où l'on considère des classes modulo deux entiers distincts, il faudra faire en sorte d'éviter les confusions.

Remarque 3.2.2 –
1. Soit x dans $\mathbb{Z}$. On a :

$$\overline{x} = \{y \in \mathbb{Z} \ ; \ x \equiv y \ (\mathrm{mod}\ n)\} = \{y \in \mathbb{Z} \ ; \ \textit{il existe } k \in \mathbb{Z} \textit{ tel que } y = x + kn\}.$$

2. Pour tout $x \in \mathbb{Z}$, $x \in \overline{x}$. En effet, $x = 0.n + x$.
3. Soit $x \in \mathbb{Z}$ et r le reste de x dans sa division euclidienne par n. Alors, il existe q dans $\mathbb{Z}$ tel que $x = qn + r$. Donc $x \in \overline{r}$.

Le troisième point de la remarque ci-dessus montre qu'un entier relatif x peut appartenir à la classe modulo n de deux entiers différents. On pourrait être temptés d'en déduire qu'il peut-être dans deux classes différentes. Il n'en est rien. Il s'avère que deux classes différentes ne peuvent pas avoir d'éléments en commun. C'est ce que précise le théorème suivant.

Théorème 3.2.3 – *Soient $x, y \in \mathbb{Z}$. Les assertions suivantes sont équivalentes :*
1. $\overline{x} \cap \overline{y} \neq \emptyset$;
2. $x \equiv y \ (\mathrm{mod}\ \ n)$;
3. $\overline{x} = \overline{y}$.

Démonstration : Montrons que la première assertion entraîne la seconde. Supposons donc que $\overline{x} \cap \overline{y} \neq \emptyset$ et notons z un entier relatif dans $\overline{x} \cap \overline{y}$. Alors, par définition des classes de congruence, x et z sont congrus modulo n et y et z sont congrus modulo n. Par transitivité de la relation de congruence, il s'ensuit que x et y sont congrus modulo n.

Montrons que la seconde assertion entraîne la troisième. On suppose donc que $x \equiv y \pmod{n}$. On va d'abord montrer que $\overline{x} \subseteq \overline{y}$. Soit $z \in \overline{x}$. Alors, z et x sont congrus modulo n et, comme x et y sont congrus modulo n, la transitivité de la relation de congruence assure que z et y sont congrues modulo n. Donc, $z \in \overline{y}$. On a montré que $\overline{x} \subseteq \overline{y}$. L'inclusion en sens inverse se montre de la même façon.

Comme enfin il est clair que la troisième assertion entraîne la première, la démonstration est terminée. ∎

Corollaire 3.2.4 –
1. Tout entier relatif appartient à une classe d'équivalence et à une seule.
2. Il y a exactement n classes d'équivalence modulo n distinctes. Ce sont les classes suivantes : $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.

Démonstration : La première assertion se déduit facilement de la remarque 3.2.2 et du théorème 3.2.3. Les détails sont laissés en exercice. Il est clair que deux éléments r, s distincts de l'ensemble $\{0, 1, \ldots, n-1\}$ ne peuvent être congrus modulo n. Donc les classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ sont deux-à-deux distinctes. De plus, pour tout entier relatif x, x est congru modulo n à un élément de $\{0, 1, \ldots, n-1\}$ (à savoir, son reste dans la division euclidienne modulo n). Donc, d'après le théorème 3.2.3, $\overline{x}$ est bien dans la liste $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. ∎

Définition 3.2.5 – *On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble dont les éléments sont les classes d'équivalence modulo n. Ainsi,*

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Exemple 3.2.6 –
1. Si $n = 1$, $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$. De plus, $\overline{0} = \mathbb{Z}$.
2. Si $n = 2$, $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$. De plus, $\overline{0} = 2\mathbb{Z}$ (ensemble des entiers pairs) et $\overline{1}$ est l'ensemble des entiers impairs.
3. Si $n = 3$, $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$. De plus, $\overline{0} = 3\mathbb{Z}$ (ensemble des entiers multiples de 3), $\overline{1} = \{1 + k.3 \ ; \ k \in \mathbb{Z}\}$ (ensemble des entiers de la forme 1 plus un multiple de 3), $\overline{2} = \{2 + k.3 \ ; \ k \in \mathbb{Z}\}$ (ensemble des entiers de la forme 2 plus un multiple de 3).

On va maintenant montrer que l'on peut munir l'ensemble $\mathbb{Z}/n\mathbb{Z}$ de deux opérations, une addition et une multiplication qui vérifient les même propriétés que l'addition et la multiplication de $\mathbb{Z}$. En des termes plus précis, on va montrer que $\mathbb{Z}/n\mathbb{Z}$ peut être muni d'une structure d'anneau. L'addition et la multiplication définies sur $\mathbb{Z}/n\mathbb{Z}$ sont en fait héritées de l'addition et de la multiplication de $\mathbb{Z}$. Il nous faut donc commencer par clarrifier le rapport qui existe entre l'addition et la multiplication dans $\mathbb{Z}$, d'une part et la relation de congruence, d'autre part.

Proposition 3.2.7 – *Soient x, x', y, y' des entiers relatifs tels que $x \equiv x' \pmod{n}$ et $y \equiv y' \pmod{n}$. Alors,*
1. $x + y \equiv x' + y' \pmod{n}$;
2. $xy \equiv x'y' \pmod{n}$.

Démonstration : Exercice. ∎

Remarque 3.2.8 – Il découle de la proposition 3.2.7 que, pour tous entiers relatifs x, x', y, y' tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, on a ;
1. $\overline{x + x'} = \overline{y + y'}$;
2. $\overline{xx'} = \overline{yy'}$.

On peut donc définir les applications suivantes

$$\begin{array}{rccc} + \ : & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & (\overline{x}, \overline{y}) & \mapsto & \overline{x+y} \end{array} \quad \text{et} \quad \begin{array}{rccc} \times \ : & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & (\overline{x}, \overline{y}) & \mapsto & \overline{xy} \end{array},$$

respectivement appelées addition et multiplication de $\mathbb{Z}/n\mathbb{Z}$.

Exemple 3.2.9 – Les tables d'addition et de multiplication de $\mathbb{Z}/7\mathbb{Z}$ sont les suivantes :

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

et

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

.

Exercice 3.2.10 – Calculer les tables d'addition et multiplication de $\mathbb{Z}/6\mathbb{Z}$.

Théorème 3.2.11 – *L'addition et la multiplication de $\mathbb{Z}/n\mathbb{Z}$ vérifient les propriétés suivantes.*
1. Pour tous $x, y, z \in \mathbb{Z}$:
1.1. $\overline{0} + \overline{x} = \overline{x}$ ($\overline{0}$ est neutre pour $+$) ;
1.2. $\overline{x} + \overline{-x} = \overline{0}$ (tout élément admet un opposé) ;
1.3. $(\overline{x} + \overline{y}) + \overline{z} = \overline{x} + (\overline{y} + \overline{z})$ (associativité de $+$) ;
1.4. $\overline{x} + \overline{y} = \overline{y} + \overline{x}$ (commutativité de $+$).
2. Pour tous $x, y, z \in \mathbb{Z}$:
2.1. $\overline{1}\overline{x} = \overline{x}$ ($\overline{1}$ est neutre pour $\times$) ;
2.2. $(\overline{x} \times \overline{y}) \times \overline{z} = \overline{x} \times (\overline{y} \times \overline{z})$ (associativité de $\times$) ;
2.3. $(\overline{x} + \overline{y}) \times \overline{z} = \overline{x} \times (\overline{y} + \overline{x} \times \overline{z})$ (distributivité de $\times$) sur $+$;
2.4. $\overline{x} \times \overline{y} = \overline{y} \times \overline{x}$ (commutativité de $\times$).

Démonstration : Exercice. ∎

3.3 Intégrité de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Considérons un ensemble A muni d'une addition et d'une multiplication (c'est-à-dire de deux applications $+ : A \times A \longrightarrow A$ et $\times : A \times A \longrightarrow A$. On dit que A est un anneau commutatif (pour ces opérations) si d'une part $+$ est associative, commutative, admet un neutre (noté 0) et si tout élément de A admet un opposé pour $+$ et si, d'autre part, $\times$ est associative, commutative, admet un neutre (noté 1) et est distributive sur $+$. Notons au passage que sur tout ensemble à un seul élément, on peut définir une structure d'anneau et une seule. L'anneau ainsi obtenu sera appelé anneau nul.

Par exemple, $\mathbb{Z}$ est un anneau commutatif et, comme le montre le théorème 3.2.11, les $\mathbb{Z}/n\mathbb{Z}$ aussi.

Définition 3.3.1 – *Soit A un anneau pour les opérations $+ : A \times A \longrightarrow A$ et $\times : A \times A \longrightarrow A$. On dit que A est intègre si il est non nul et si le produit de deux éléments non nuls (c'est-à-dire distints de 0) de A est non nul.*

Exemple 3.3.2 –
1. L'anneau $\mathbb{Z}$ des entiers relatifs est intègre.
2. Si l'on observe la table de multiplication de $\mathbb{Z}/7\mathbb{Z}$ dressée plus haut, on constate facilement que la seule possibilité pour qu'un produit soit nul est que l'un des facteurs soit nul. Donc, L'anneau $\mathbb{Z}/7\mathbb{Z}$ est intègre.
3. La situation est radicalement différente pour $\mathbb{Z}/6\mathbb{Z}$. En effet, les éléments de $\mathbb{Z}/6\mathbb{Z}$ sont $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$. Donc, $\overline{2}$ et $\overline{3}$ sont non nuls. Pourtant $\overline{2}.\overline{3} = \overline{2.3} = \overline{6} = \overline{0}$ Ainsi, $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre.
4. Plus généralement, si n n'est pas premier, il existe $k, l \in \{1, \ldots, n-1\}$ tels que $n = kl$. Comme la liste exhaustive des n éléments de $\mathbb{Z}/n\mathbb{Z}$ est $\overline{0}, \overline{1}, \ldots, \overline{n-1}$, $\overline{k}$ et $\overline{l}$ ne sont pas nuls. Pourtant $\overline{k}.\overline{l} = \overline{kl} = \overline{n} = \overline{0}$. Donc, si n n'est pas premier, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

Le phénomène observé au second et troisième points de l'exemple 3.3.2 ci-dessus conduit naturellement à la question suivante : à quelle condition portant sur n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il intègre ?

Le théorème ci-dessous répond à cette question.

Théorème 3.3.3 – *Soit n un nombre premier.*
1. Tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ admet un inverse pour la multiplication. C'est-à-dire que, pour tout $a \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \neq \overline{0}$, il existe $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $a.b = \overline{1}$.
2. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre.

Démonstration : 1. Puisque n est premier, en vertu du théorème 2.3.8, il est premier avec tous les éléments de $\{1, 2, \ldots, n-1\}$. Soit $a \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \neq \overline{0}$. Alors, il existe $x \in \{1, 2, \ldots, n-1\}$ tel que $a = \overline{x}$. Et, comme x et n sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $ux + vn = 1$. On a donc $\overline{u}.\overline{x} = \overline{1}$, ce qui montre que a est bien inversible.
2. On doit montrer que le produit de deux éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ est non nul. Soient a, b deux tels éléments. Supposons au contraire que $ab = \overline{0}$. D'après le point 1, il existe des éléments $c, d \in \mathbb{Z}/n\mathbb{Z}$ tels que $ac = bd = \overline{1}$. De $ab = \overline{0}$, on tire donc que $\overline{1} = abcd = \overline{0}$, ce qui est faux. Donc $ab \neq \overline{0}$. ∎

A ce stade, il est commode d'introduire la notion de corps. Considérons un ensemble A muni d'une addition et d'une multiplication (c'est-à-dire de deux applications $+ : A \times A \longrightarrow A$ et $\times : A \times A \longrightarrow A$. On dit que A est un corps si A est un anneau commutatif (pour ces opérations), si A a au moins 2 éléments distincts et si, tout élément non nul de A admet un inverse pour la multiplication (autrement dit, pour tout $x \in A \setminus \{0\}$, il existe $y \in A$ tel que $xy = 1$, ou 1 désigne le neutre de la multiplication).

Avec ce vocabulaire, ce qui précède assure qu'on a le théorème suivant.

Théorème 3.3.4 – *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier et, si n est premier, $\mathbb{Z}/n\mathbb{Z}$ est un corps.*

4 Appendice : construction de $\mathbb{Z}$.

Dans cette partie, on montre comment l'on peut construire $\mathbb{Z}$ à partir de $\mathbb{N}$.

La construction rigoureuse de $\mathbb{Z}$ n'est pas très éloignée de l'idée intuitive que l'on a de la notion d'entier négatif. L'idée qui mène à la création de nombres entiers négatifs est la suivante. On sait retrancher un petit entier (par exemple 7) à un entier plus grand (par exemple 12). Ainsi, on a obtenu 5 à partir du couple $(12, 7)$. Bien sûr, on pourrait obtenir 5 à partir du couple $(24, 19)$. Mais, si l'on reste dans $\mathbb{N}$, on ne peut pas retrancher 12 à 7. L'introduction des nombres entiers négatifs a pour but de palier à ce manque. On est alors tenté de définir -5 par le biais du couple $(7, 12)$. Mais alors, se pose immédiatement le problème que l'on peut tout aussi naturellement définir -5 à l'aide du couple $(11, 16)$.

C'est exactement ce point de vue que l'on met en oeuvre pour définir $\mathbb{Z}$ à partir de $\mathbb{N}$. Ainsi, les entiers négatifs seront construits en considérant des couples d'entiers naturels et l'on introduira une *relation d'équivalence* permettant d'identifier (de force) les couples dont on pense intuitivement qu'ils doivent conduire au même nombre négatif, comme $(7, 12)$ et $(11, 16)$ par exemple.

4.1 Définition de $\mathbb{Z}$.

On procède maintenant à cette construction rigoureuse.

On considère l'ensemble $\mathbb{N} \times \mathbb{N}$ des couples d'entiers naturels. Sur cet ensemble, on définit une *relation binaire*, c'est-à-dire un moyen de relier certains éléments de $\mathbb{N} \times \mathbb{N}$. Plus précisément, on définit la relation binaire $\mathcal{R}$ de la façon suivante : si (a, a') et (b, b') sont des éléments de $\mathbb{N} \times \mathbb{N}$, on dit que (a, a') et (b, b') sont reliés par $\mathcal{R}$, ce que l'on note $(a, a')\,\mathcal{R}\,(b, b')$, si $a + b' = a' + b$.

Par exemple, $(5, 12)\,\mathcal{R}\,(12, 19)$ (qui exprime que $(5, 12)$ et $(12, 19)$ sont reliés par $\mathcal{R}$). Mais, $(7, 12)\ \mathcal{R}\,(10, 19)$ (qui exprime que $(7, 12)$ et $(10, 19)$ ne sont pas reliés par $\mathcal{R}$).

Une relation binaire est appelée une *relation d'équivalence* si elle est réflexive, symétrique et transitive (au sens ci-dessous). La proposition qui suit exprime donc que la relation $\mathcal{R}$ définie ci-dessus est une relation d'équivalence.

Proposition 4.1.1 –
1. Pour tout $(a, a') \in \mathbb{N} \times \mathbb{N}$, $(a, a')\,\mathcal{R}(a, a')$ (réflexivité).
2. Pour tous $(a, a'), (b, b') \in \mathbb{N} \times \mathbb{N}$, si $(a, a')\,\mathcal{R}(b, b')$, alors $(b, b')\mathcal{R}(a, a')$ (symétrie).
3. Pour tous $(a, a'), (b, b'), (c, c') \in \mathbb{N} \times \mathbb{N}$, si $(a, a')\,\mathcal{R}(b, b')$, et $(b, b')\mathcal{R}(c, c')$, alors $(a, a')\mathcal{R}(c, c')$ (transitivité).

Démonstration : 1. Soit $(a, a') \in \mathbb{N} \times \mathbb{N}$. Il est clair que $a + a' = a' + a$ (puisque l'addition dans $\mathbb{N}$ est commutative). Donc, $(a, a')\,\mathcal{R}(a, a')$.
2. Soient $(a, a'), (b, b') \in \mathbb{N} \times \mathbb{N}$. Supposons que $(a, a')\,\mathcal{R}(b, b')$, alors $a + b' = a' + b$. Il s'ensuit que $b + a' = b' + a$ (à nouveau pas commutativité de l'addition dans $\mathbb{N}$), ce qui exprime que $(b, b')\mathcal{R}(a, a')$.
3. Soient $(a, a'), (b, b'), (c, c') \in \mathbb{N} \times \mathbb{N}$. Supposons que $(a, a')\,\mathcal{R}(b, b')$ et $(b, b')\mathcal{R}(c, c')$. On a donc $a + b' = a' + b$ et $b + c' = b' + c$. Il s'ensuit que $(a + b') + (b + c') = (a' + b) + (b' + c)$ et donc que $a + c' = a' + c$ (ici, on a utilisé l'associativité, la commutativité et la règle de simplification

de l'addition dans $\mathbb{N}$). Ainsi, $(a,a')\mathcal{R}(c,c')$ (transitivité). ∎

On va maintenant montrer qu'à l'aide de la relation $\mathcal{R}$ on peut "décomposer" $\mathbb{N}\times\mathbb{N}$ en sous-ensembles, les *classes d'équivalence* pour la relation $\mathcal{R}$, de sorte que tout élément de $\mathbb{N}\times\mathbb{N}$ soit dans une classe et dans une seule.

Définition 4.1.2 – *Soit $(x,x')\in\mathbb{N}\times\mathbb{N}$. La classe d'équivalence de (x,x') pour la relation $\mathcal{R}$ est le sous-ensemble de $\mathbb{N}\times\mathbb{N}$, noté $\overline{(x,x')}$ et défini par*

$$\overline{(x,x')}=\{(a,a')\in\mathbb{N}\times\mathbb{N}\,;(a,a')\mathcal{R}(x,x')\}.$$

Remarque 4.1.3 –
1. Ainsi, par définition, la classe d'équivalence d'un élément (x,x') de $\mathbb{N}\times\mathbb{N}$ est l'ensemble des éléments de $\mathbb{N}\times\mathbb{N}$ qui sont reliés à (x,x') par la relation $\mathcal{R}$.
2. Comme la relation $\mathcal{R}$ est réflexive, tout élément de $\mathbb{N}\times\mathbb{N}$ appartient à sa classe déquivalence : pour tout $(x,x')\in\mathbb{N}\times\mathbb{N}$, $(x,x')\in\overline{(x,x')}$.

Le lemme suivant est très important pour la suite.

Lemme 4.1.4 – *Soient (x,x') et (y,y') des éléments de $\mathbb{N}\times\mathbb{N}$. Les assertions suivantes sont équivalentes :*
1. $(x,x')\mathcal{R}(y,y')$ *;*
2. $(x,x')\in\overline{(y,y')}$ *;*
3. $\overline{(y,y')}\in\overline{(x,x')}$ *;*
4. $\overline{(x,x')}=\overline{(y,y')}$.

Démonstration : La définition de classe d'équivalence assure que les assertions 1 et 2 d'une part et 1 et 3 d'autre part sont équivalentes. Ainsi, les assertions 1, 2 et 3 sont équivalentes. D'après le second point de la remarque 4.1.3, il est clair que l'assertion 4 implique l'assertion 2, et donc l'assertion 1.

A présent, supposons l'assertion 1 vérifiée : $(x,x')\mathcal{R}(y,y')$. Si $(z,z')\in\overline{(y,y')}$, alors $(y,y')\mathcal{R}(z,z')$. Par transitivité on a donc que $(z,z')\mathcal{R}(x,x')$ qui assure que $(z,z')\in\overline{(x,x')}$. Ainsi, on a montré que si l'assertion 1 est vérifiée, on a $\overline{(x,x')}\supseteq\overline{(y,y')}$. En procédant de même, on trouve que $\overline{(x,x')}\subseteq\overline{(y,y')}$. Finalement, on a montré que si l'assertion 1 est vérifiée, l'assertion 4 l'est.

La démonstration est terminée. ∎

La remarque suivante permet de clarifier la situation.

Remarque 4.1.5 –
1. Soit $(x,x')\in\mathbb{N}\times\mathbb{N}$. Deux cas sont possibles.
– Ou bien $x\geq x'$. Alors, par définition de la relation d'ordre dans $\mathbb{N}$, il existe $n\in\mathbb{N}$ tel que $x=x'+n$. On peut alors facilement vérifier que $(x,x')\mathcal{R}(n,0)$.
– Ou bien $x<x'$. Alors, par définition de la relation d'ordre dans $\mathbb{N}$, il existe $n\in\mathbb{N}^*$ tel que $x'=x+n$. On peut alors facilement vérifier que $(x,x')\mathcal{R}(0,n)$.
2. Ainsi, la liste exhaustive des classes d'équivalences de $\mathbb{N}\times\mathbb{N}$ pour la relation $\mathcal{R}$ est :

$$\ldots,\overline{(0,3)},\overline{(0,2)},\overline{(0,1)},\overline{(0,0)},\overline{(1,0)},\overline{(2,0)},\overline{(3,0)},\ldots$$

3. De plus, la liste ci-dessus est une liste sans répétition, c'est-à-dire que les classes d'équivalence qui y apparaissent sont deux-à-deux distinctes. (Vérification en exercice.)

L'ensemble $\mathbb{Z}$ des entiers relatif peut maintenant être défini.

Définition 4.1.6 – *L'ensemble $\mathbb{Z}$ est l'ensemble dont les éléments sont les classes d'équivalence de $\mathbb{N}\times\mathbb{N}$ pour la relation $\mathcal{R}$. Ses éléments sont appelés les entiers relatifs.*

Remarque 4.1.7 – Compte tenu de ce qui précède, on a donc la liste exhaustive et sans répétition des éléments de $\mathbb{Z}$:

$$\mathbb{Z} = \{\ldots, \overline{(0,3)}, \overline{(0,2)}, \overline{(0,1)}, \overline{(0,0)}, \overline{(1,0)}, \overline{(2,0)}, \overline{(3,0)}, \ldots\}$$

Attention, il faut bien prendre garde que, pour tout $(x,x')\in\mathbb{N}\times\mathbb{N}$, $\overline{(x,x')}\in\mathbb{Z}$. Cependant, la remarque 4.1.5 assure que, même si (x,x') n'est pas dans la liste

$$\ldots, (0,3), (0,2), (0,1), (0,0), (1,0), (2,0), (3,0), \ldots,$$

sa classe d'équivalence, elle, est dans la liste

$$\ldots, \overline{(0,3)}, \overline{(0,2)}, \overline{(0,1)}, \overline{(0,0)}, \overline{(1,0)}, \overline{(2,0)}, \overline{(3,0)}, \ldots.$$

Par exemple, $\overline{(7,12)} = \overline{(0,5)}$.

4.2 Opérations sur $\mathbb{Z}$.

On va maintenant montrer que $\mathbb{Z}$ peut être muni d'une addition et d'une multiplication.

Comme on a vu que l'ensemble $\mathbb{Z}$ est donné par

$$\mathbb{Z} = \{\ldots, \overline{(0,3)}, \overline{(0,2)}, \overline{(0,1)}, \overline{(0,0)}, \overline{(1,0)}, \overline{(2,0)}, \overline{(3,0)}, \ldots\},$$

pour définir une opération sur $\mathbb{Z}$, il suffit de la définir sur les éléments de cette liste. Cependant, si l'on essaie de s'y prendre de cette façon, on s'apperçoit vite qu'on a des ennuis. Ainsi, par exemple, si l'on se réfère à l'intuition, on voudrait que $\overline{(0,7)}+\overline{(5,0)} = \overline{(0,2)}$ et que $\overline{(0,5)}+\overline{(7,0)} = \overline{(2,0)}$. Ainsi, la position du coefficient non nul dans le résultat dépend d'où se trouve le plus grand coefficient non nul dans les sommants. Bref, une telle approche amènerait à distinguer de multiples cas et serait illisible.

On procède un peu différemment. Soient deux éléments de $\mathbb{Z}$, c'est-à-dire deux classes d'équivalences, que l'on veut additionner. On va prendre, au hasard, un élément (x,x') dans la première classe et un élément (y,y') dans la seconde. Comme on l'a déjà remarqué, la première classe est donc $\overline{(x,x')}$ et la seconde est $\overline{(y,y')}$. On est alors tenté de dire que la somme de ces deux éléments est $\overline{(x+x',y+y')}$. Mais, là, se pose un problème. Le choix du (x,x') dans la première classe et du (y,y') dans la seconde peut-il influer sur le résultat ? Si c'est le cas, notre définition pour l'addition de deux éléments de $\mathbb{Z}$ n'a pas de sens. Le lemme suivant montre que ce choix n'a pas d'influence.

Lemme 4.2.1 – *Soient (x_1,x_1'), (x_2,x_2'), (y_1,y_1') et (y_2,y_2') des éléments de $\mathbb{N}\times\mathbb{N}$. Si (x_1,x_1') et (x_2,x_2') sont dans la même classe et si (y_1,y_1') et (y_2,y_2') sont dans la même classe, alors $(x_1+y_1,x_1'+y_1')$ et $(x_2+y_2,x_2'+y_2')$ sont dans la même classe.*

Démonstration : Puisque (x_1,x_1') et (x_2,x_2') sont dans la même classe, on a $x_1+x_2' = x_1'+x_2$. Puisque (y_1,y_1') et (y_2,y_2') sont dans la même classe, on a $y_1+y_2' = y_1'+y_2$. Il s'ensuit que $(x_1+y_1)+(x_2'+y_2') = (x_1'+y_1')+(x_2+y_2)$, ce qui exprime que $(x_1+y_1,x_1'+y_1')$ et $(x_2+y_2,x_2'+y_2')$

sont dans la même classe. ∎

Le problème de choix évoqué ci-dessus ne se pose donc pas et l'on définit l'addition de la façon suivante.

Définition 4.2.2 – *On appelle addition sur $\mathbb{Z}$, notée $+$, l'opération*

$$\begin{array}{rccc} + & : & \mathbb{Z}\times\mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & & (\overline{(x,x')},\overline{(y,y')}) & \mapsto & \overline{(x+x',y+y')} \end{array}$$

On a alors la propriété suivante. Sa démonstration est facile et elle est donc laissée en exercice (voir tout de même la remarque 4.2.4 pour des précisions).

Proposition 4.2.3 – *L'addition de $\mathbb{Z}$ est commutative et associative. De plus, $\overline{(0,0)}$ est neutre pour l'addition de $\mathbb{Z}$. Enfin, tout élément de $\mathbb{Z}$ admet un opposé pour l'addition.*

Démonstration : Exercice. ∎

Remarque 4.2.4 –
1. La proposition 4.2.3 exprime en fait que $\mathbb{Z}$ est un groupe commutatif de neutre $\overline{(0,0)}$ pour la loi $+$ ci-dessus.
2. Déterminons l'opposé d'un élément de $\mathbb{Z}$. Tout élément de $\mathbb{Z}$ est une classe d'équivalence pour la relation $\mathcal{R}$. Ainis, si l'on considère un élément de $\mathbb{Z}$, il existe un couple $(x,x')\in\mathbb{N}\times\mathbb{N}$ tel que cet élément soit $\overline{(x,x')}$. Mais alors, on a $\overline{(x,x')}+\overline{(x',x)}=\overline{(x+x',x'+x)}=\overline{(0,0)}$. Ceci montre que $\overline{(x,x')}$ admet $\overline{(x',x)}$ pour opposé.

On définit, à présent, une multiplication dans $\mathbb{Z}$. Le même problème de choix se pose que pour l'addition. Il est réglé par le lemme suivant qui est donc l'analogue du lemme 4.2.1.

Lemme 4.2.5 – *Soient (x_1,x_1'), (x_2,x_2'), (y_1,y_1') et (y_2,y_2') des éléments de $\mathbb{N}\times\mathbb{N}$. Si (x_1,x_1') et (x_2,x_2') sont dans la même classe et si (y_1,y_1') et (y_2,y_2') sont dans la même classe, alors $(x_1y_1+x_1'y_1',x_1y_1'+x_1'y_1)$ et $(x_2y_2+x_2'y_2',x_2y_2'+x_2'y_2)$ sont dans la même classe.*

Démonstration : Puisque (x_1,x_1') et (x_2,x_2') sont dans la même classe, et puisque (y_1,y_1') et (y_2,y_2') sont dans la même classe, on a

$$x_1+x_2'=x_1'+x_2 \quad (1) \qquad \text{et} \qquad y_1+y_2'=y_1'+y_2 \quad (2).$$

L'équation (1) multipliée par y_1, l'équation (1) multipliées par y_1' (et lue à l'envers), l'équation (2) multipliée par x_2 et l'équation (2) multipliée par x_2' (et lue à l'envers) donnent respectivement

$$\begin{array}{rcl} x_1y_1+x_2'y_1 &=& x_1'y_1+x_2y_1, \\ x_1'y_1'+x_2y_1' &=& x_1y_1'+x_2'y_1', \\ x_2y_1+x_2y_2' &=& x_2y_1'+x_2y_2, \\ x_2'y_1'+x_2'y_2 &=& x_2'y_1+x_2'y_2'. \end{array}$$

En additionnant ces quatres égalités et en simplifiant, on trouve $(x_1y_1+x_1'y_1')+(x_2y_2'+x_2'y_2)=(x_1y_1'+x_1'y_1)+(x_2y_2+x_2'y_2')$, ce qui exprime que $(x_1y_1+x_1'y_1',x_1y_1'+x_1'y_1)$ et $(x_2y_2+x_2'y_2',x_2y_2'+x_2'y_2)$ sont dans la même classe. ∎

On peut donc définir la multiplication de la façon suivante.

Définition 4.2.6 – *On appelle multiplication sur $\mathbb{Z}$, notée $\times$, l'opération*

$$\begin{array}{rccc} \times & : & \mathbb{Z}\times\mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & & \overline{((x,x'),(y,y'))} & \mapsto & \overline{(xy+x'y',xy'+x'y)} \end{array}.$$

On a alors la propriété suivante. Sa démonstration est facile et elle est donc laissée en exercice.

Proposition 4.2.7 – *La multiplication de $\mathbb{Z}$ est commutative, associative et distributive sur l'addition. De plus, $\overline{(1,0)}$ est neutre pour la multiplication de $\mathbb{Z}$.*

Démonstration : Exercice. ∎

Remarque 4.2.8 –
La proposition 4.2.7 jointe à la proposition 4.2.3 exprime en fait que $\mathbb{Z}$ est un anneau commutatif de neutre $\overline{(0,0)}$ pour la loi $+$ et de neutre $\overline{(1,0)}$ pour la loi $\times$.

La proposition suivante est importante. Elle assure que l'anneau $\mathbb{Z}$ est intègre.

Proposition 4.2.9 – *L'anneau $\mathbb{Z}$ est intègre. C'est-à-dire que le produit de deux éléments de $\mathbb{Z}$ différents de $\overline{(0,0)}$ est différent de $\overline{(0,0)}$.*

Démonstration : Soient x et y deux éléments de $\mathbb{Z}$, différents de $\overline{(0,0)}$. A la remarque 4.1.7, on a vu que

$$\mathbb{Z}=\{\ldots,\overline{(0,3)},\overline{(0,2)},\overline{(0,1)},\overline{(0,0)},\overline{(1,0)},\overline{(2,0)},\overline{(3,0)},\ldots\},$$

cette liste étant sans répétition. Trois cas de figure se présentent donc.
Premier cas. Il existe $m,n\in\mathbb{N}\setminus\{0\}$ tels que $x=\overline{(m,0)}$ et $y=\overline{(n,0)}$. Alors, $xy=\overline{(mn,0)}$. Comme m et n sont des éléments non nuls de $\mathbb{N}$, $mn\neq 0$, ce qui assure que $xy\neq\overline{(0,0)}$.
Deuxième cas. Il existe $m,n\in\mathbb{N}\setminus\{0\}$ tels que $x=\overline{(0,m)}$ et $y=\overline{(0,n)}$. Alors, $xy=\overline{(mn,0)}$. Comme précédemment, cela assure que $xy\neq\overline{(0,0)}$.
Troisième cas. Il existe $m,n\in\mathbb{N}\setminus\{0\}$ tels que $x=\overline{(m,0)}$ et $y=\overline{(0,n)}$. Alors, $xy=\overline{(0,mn)}$. A nouveau, on trouve que $xy\neq\overline{(0,0)}$. ∎

4.3 L'injection canonique de $\mathbb{N}$ dans $\mathbb{Z}$.

Avec la construction de $\mathbb{Z}$ précédemment décrite, il est clair que $\mathbb{N}$ n'est pas, contrairement à ce que souhaiterait l'intuition, un sous-ensemble de $\mathbb{Z}$. Cependant, on peut identifier $\mathbb{N}$ à un sous-ensemble de $\mathbb{Z}$. C'est ce que l'on montre maintenant.

Pour ce faire, on considère l'application :

$$\begin{array}{rccc} \iota & : & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & & n & \mapsto & \overline{(n,0)} \end{array}.$$

On a alors la proposition suivante.

Proposition 4.3.1 –
1. L'application ι est injective.
2. L'application ι respecte les opérations $+$ et $\times$, c'est-à-dire que : $\forall m,n\in\mathbb{N}$, $\iota(m+n)=\iota(m)+\iota(n)$ et $\iota(mn)=\iota(m)\iota(n)$.
3. Les éléments $\iota(0)$ et $\iota(1)$ sont les neutres respectifs des opérations $+$ et $\times$ de $\mathbb{Z}$.
4. Pour tout élément x de $\mathbb{Z}$, il existe $n\in\mathbb{N}$ tel que $x=\iota(n)$ ou $x=-\iota(n)$.

Démonstration : 1. L'injectivité de ι se déduit immédiatement de la remarque 4.1.7.
2. Soient $m, n \in \mathbb{N}$. Alors, compte tenu de la définition de l'addition et de la multiplication dans $\mathbb{Z}$, on a $\iota(m+n) = \overline{(m+n,0)} = \overline{(m,0)} + \overline{(n,0)} = \iota(m) + \iota(n)$ et $\iota(mn) = \overline{(mn,0)} = \overline{(m,0)}\,\overline{(n,0)} = \iota(m)\iota(n)$.
3. Il est clair que $\iota(0) = \overline{(0,0)}$ et $\iota(1) = \overline{(1,0)}$ qui sont les neutres respectifs des opérations $+$ et $\times$ de $\mathbb{Z}$.
4. Soit x dans $\mathbb{Z}$. A la remarque 4.1.7, on a vu qu'il existe $n \in \mathbb{N}$ tel que $x = \overline{(n,0)} = \iota(n)$ ou $x = \overline{(0,n)} = -\overline{(n,0)} = -\iota(n)$. ∎

On montre maintenant comment on peut identifier un $\mathbb{N}$ à un sous-ensemble de $\mathbb{Z}$.

Remarque 4.3.2 –
1. Le premier point de la propriété 4.3.1 assure que l'image, $\iota(\mathbb{N})$, de ι dans $\mathbb{Z}$ est en bijection avec $\mathbb{N}$. Cette image n'est autre que

$$\iota(\mathbb{N}) = \{\overline{(0,0)}, \overline{(1,0)}, \overline{(2,0)}, \ldots\}.$$

On peut donc identifier les ensembles $\mathbb{N}$ et $\iota(\mathbb{N})$. Ainsi, tout entier naturel $n \in \mathbb{N}$ sera confondu avec son image $\overline{(n,0)}$, ce qui signifie que, par abus de langage, on notera n l'élément $\overline{(n,0)}$ de $\mathbb{Z}$.
2. Bien sûr, une telle identification peut entrainer des confusions et des ambigüités. Ainsi, pour deux entiers naturels m et n, l'écriture $m+n$ a maintenant deux interprétations possibles. Elle peut signifier l'addition de m et n dans $\mathbb{N}$, ou l'addition de $\iota(m)$ et $\iota(n)$ dans $\mathbb{Z}$. Mais, compte tenu du second point de la proposition 4.3.1, on a $\iota(m) + \iota(n) = \iota(m+n)$ qui, dans l'abus de langage ci-dessus, s'identifie à $m+n$. Ainsi, quelle que soit la façon d'interpréter $m+n$, on obtient (à identification près) le même élément. Et, toujours d'après la proposition 4.3.1, la même remarque s'applique à la multiplication. Si on ajoute à cela le troisième point de la proposition 4.3.1, on obtient que les additions et multiplications de $\mathbb{N}$ et $\mathbb{Z}$ sont compatibles avec l'identification ci-dessus.
3. Conformément au quatrième point de la proposition 4.3.1, pour tout élément x de $\mathbb{Z}$, il existe $n \in \mathbb{N}$ tel que $x = \iota(n)$ ou $x = -\iota(n)$. Avec les conventions adoptées au second point de la présente remarque portant sur l'identification de $\mathbb{N}$ comme sous-ensemble de $\mathbb{Z}$, on obtient une nouvelle description de $\mathbb{Z}$:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\},$$

la liste ci-dessus étant sans répétition. On retrouve donc la représentation intuitive habituelle de $\mathbb{Z}$.

5 *Exercices.*

§A - Propriétés élémentaires de $\mathbb{Z}$, équations diophantiennes.

Exercice 5.1 – **Equations diophantiennes.**
1. Soient $a, b, c \in \mathbb{Z}$. Le but de cette question est l'étude des solutions, dans $\mathbb{Z}$, de l'équation $ax + by = c$. On note d le p.g.c.d. positif de a et b et on pose $a = da'$ et $b = db'$. On pose $S = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \,|\, ax + by = c\}$. Montrer que :
(i) Si d ne divise pas c alors $S = \emptyset$;
(ii) si d divise c alors S est non vide, et $S = \{(x_0 - kb', y_0 + ka'),\ k \in \mathbb{Z}\}$ où (x_0, y_0) est une solution quelconque de l'équation $ax + by = c$.
2. Résoudre dans $\mathbb{Z}$ l'équation $31x + 56y = 4$.

§B - Le groupe $\mathbb{Z}/n\mathbb{Z}$.

Exercice 5.2 –
1. Soit G un groupe et $f : \mathbb{Z} \longrightarrow G$ un morphisme de groupes.
1.1 On suppose que $n \in \mathbb{Z}$ est dans le noyau de f. Montrer qu'il existe un morphisme de groupes $g : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ et un seul, tel que $f = g \circ \pi$, où π est la projection canonique $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$..
1.2. On reprend les notations de 1.1. Montrer que si $\ker f = n\mathbb{Z}$, alors g est injective.
1.3. On reprend les notations de 1.1. Montrer que si f est surjective, alors g l'est aussi.
2. Soit G un groupe.
2.1. Montrer que, pour tout élément g de G, l'applcation $\mathbb{Z} \longrightarrow G$, $n \mapsto g^n$ est un morphisme de groupes. Décrire son image et son noyau.
2.2. Montrer que si G est monogène, alors : soit il est d'ordre infini et isomorphe à $\mathbb{Z}$, soit d'ordre fini $d \in \mathbb{N}^*$ et isomorphe à $\mathbb{Z}/d\mathbb{Z}$.

Exercice 5.3 – Soit $n \in \mathbb{N}^*$. Déterminer tous les générateurs des groups monogènes $\mathbb{Z}/n\mathbb{Z}$ et μ_n.

Exercice 5.4 – Montrer que les groupes $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sont abéliens, d'ordre 4 mais non isomorphes.

§C - L'anneau $\mathbb{Z}/nZ$.

Exercice 5.5 –
1. Soit $n \in \mathbb{N}^*$. Déterminer les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.
2. La classe modulo 85 de 49 est-elle un élément inversible de $\mathbb{Z}/85\mathbb{Z}$? Dans l'affirmative, calculer son inverse.

Exercice 5.6 – Dans cet exercice, on pourra utiliser l'exercice 5.2.
1. Soit A un anneau et $f : \mathbb{Z} \longrightarrow A$ un morphisme d'anneaux.
1.1 On suppose que $n \in \mathbb{Z}$ est dans le noyau de f. Montrer qu'il existe un morphisme d'anneaux $g : \mathbb{Z}/n\mathbb{Z} \longrightarrow A$ et un seul, tel que $f = g \circ \pi$, où π est la projection canonique $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$.
1.2. On reprend les notations de 1.1. Montrer que si $\ker f = n\mathbb{Z}$, alors g est injective.
1.3. On reprend les notations de 1.1. Montrer que si f est surjective, alors g l'est aussi.
2. Application : caractéristique d'un anneau.
Soit A un anneau. Montrer que l'application $\mathbb{Z} \longrightarrow A$, $n \mapsto n.1_A$ est un morphisme d'anneaux. On rappelle que, pour $n \in \mathbb{Z}$ et $a \in A$, on pose $n.a = a + \ldots + a$ (n-fois) si $n > 0$, $n.1_A = (-a) + \ldots + (-a)$ ($-n$-fois) si $n < 0$ et $0.1_A = 0_A$. Il existe un unique entier positif p tel que $\ker f = p\mathbb{Z}$. Cet entier s'appelle la caractéristique de A.

Exercice 5.7 – Résoudre, dans $\mathbb{Z}$, les systèmes de congruences suivants :

$$\begin{cases} x \equiv 1 \bmod 5\mathbb{Z} \\ x \equiv 2 \bmod 3\mathbb{Z} \end{cases} \quad \text{et} \quad \begin{cases} x \equiv 2 \bmod 17\mathbb{Z} \\ x \equiv 11 \bmod 28\mathbb{Z} \end{cases}.$$

Exercice 5.8 – **Fonction indicatrice d'Euler.**
On considère l'application $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}$, appelée fonction indicatrice d'Euler, qui à tout entier $n \geq 2$ associe le cardinal du groupe $(\mathbb{Z}/n\mathbb{Z})^*$ des unités de l'anneau $\mathbb{Z}/n\mathbb{Z}$ et telle que $\varphi(1) = 1$. Le but de cet exercice est l'étude de φ.
1. Soient n et m deux entiers premiers entre eux.
1.1. On considère l'application $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/mZ$, $x \mapsto x + n\mathbb{Z}, x + m\mathbb{Z}$. Montrer que cette

application est un morphisme d'anneaux de noyau $mn\mathbb{Z}$.
1.2. En déduire que les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes.
1.3. Trouver un contre-exemple à ce résultat si l'on ne suppose pas n et m premiers entre eux.
1.4. Montrer que les groupes $(\mathbb{Z}/nm\mathbb{Z})^*$ et $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ sont isomorphes.
2. Soit $n \in \mathbb{N}^*$ tel que $n = \prod_{1 \leq i \leq k} p_i^{r_i}$ où $p_1, \ldots, p_k$ sont des nombres premiers distincts et $r_1, \ldots, r_k$ des entiers strictement positifs.
2.1. Montrer que les groupes $(\mathbb{Z}/n\mathbb{Z})^*$ et $\prod_{1 \leq i \leq k} (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*$ sont isomorphes.
2.2. Montrer que $\varphi(n) = n \times \prod_{1 \leq i \leq k} (1 - \frac{1}{p_i})$.
3. Une caractérisation de φ.
3.1. Montrer, par récurrence sur n, que, pour tout $n \in \mathbb{N}^*$, on a l'identité d'Euler :

$$n = \sum_{d|n} \varphi(d).$$

3.2. Montrer que, si $\chi : \mathbb{N}^* \longrightarrow \mathbb{N}$ est une application telle que, pour tout $n \in \mathbb{N}^*$, $n = \sum_{d|n} \chi(d)$, alors $\chi = \varphi$.

§D - Quelques grands classiques.

Exercice 5.9 – Le petit théorème de Fermat.
Le petit théorème de Fermat peut s'énoncer de deux façons différentes :
(i) soit p un nombre premier, pour tout $a \in \mathbb{Z}$ non divisible par p, p divise $a^{p-1} - 1$;
(ii) soit p un nombre premier, pour tout $a \in \mathbb{Z}$, p divise $a^p - a$.
1. Montrer que les assertions (i) et (ii) sont équivalentes.
2. Une démonstration élémentaire (due à Euler).
2.1. Montrer que, pour tout $1 \leq k \leq p-1$, p divise $\binom{p}{k}$.
2.2. En déduire que, pour tous $x, y \in \mathbb{Z}$, p divise $(x+y)^p - (x^p + y^p)$.
2.3. Conclure, en utilisant une récurrence.
3. Une démonstration plus sophistiquée (due à Gauss).
Montrer (i) en utilisant le théorème de Lagrange (cf. l'exercice 1.3.5 de la section X.1).
4. Quelques applications.
4.1. Montrer que 13 divise $2^{70} + 3^{70}$.
4.2. Quel est le reste de la division euclidienne de 247^{349} par 7 ?

Exercice 5.10 – Le théorème de Wilson.
Le théorème de Wilson affirme que, pour un entier $p \in \mathbb{N} \setminus \{0, 1\}$, les assertions suivantes sont équivalentes :
(i) p est un nombre premier ;
(ii) $(p-1)! + 1 \equiv 0 \,(\mathrm{mod}\, p\mathbb{Z})$.
Le but de cet exercice est d'en donner une démonstration.
1. La preuve de (i) implique (ii) due à Gauss.
1.1. On suppose p impair.
1.1.1. Déterminer les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ (groupe des unités de $\mathbb{Z}/p\mathbb{Z}$) qui sont leur propre inverse.
1.1.2. On considère la projection canonique $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$, $x \mapsto \overline{x}$. Montrer que, dans $\mathbb{Z}/p\mathbb{Z}$, on a l'identié suivante : $\overline{1} \ldots \overline{p-1} = \overline{-1}\,\overline{1}$.
1.2. Conclure.
2. Montrer que (ii) implique (i).

Partie IV

Les nombres complexes.

1 Le corps $\mathbb{C}$ des nombres complexes.

On définit sur $\mathbb{R}^2$ les opérations suivantes, appelées respectivement addition et multiplication de $\mathbb{R}^2$:

$$\begin{array}{rccc} + & : & \mathbb{R}^2 \times \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & & ((x,y),(x',y')) & \mapsto & (x+x', y+y') \end{array}$$

et

$$\begin{array}{rccc} \times & : & \mathbb{R}^2 \times \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & & ((x,y),(x',y')) & \mapsto & (xx'-yy', xy'+yx') \end{array} .$$

Théorème 1.1 – *L'ensemble $\mathbb{R}^2$ muni de l'addition et de la multiplication définies ci-dessus est un corps commutatif.*

Démonstration : 1. Le fait que l'addition soit commutative et associative est un exercice facile. De même, on vérifie facilement que $(0,0)$ est un neutre pour l'addition et que, pour tout $(x,y) \in \mathbb{R}^2$, l'élément $(-x,-y)$ est un opposé.
2. Le fait que la multiplication de $\mathbb{R}^2$ soit commutative et admette $(1,0)$ comme élément neutre se vérifie facilement.

Montrons que la multiplication est associative. Soient (x,y), (x',y') et (x'',y'') des éléments de $\mathbb{R}^2$. Alors, on a :

$$\begin{array}{rcl} ((x,y).(x',y')).(x'',y'') & = & (xx'-yy', xy'+yx').(x'',y'') \\ & = & ((xx'-yy')x''-(xy'+yx')y'', (xx'-yy')y''+(xy'+yx')x'') \\ & = & (xx'x''-yy'x''-xy'y''-yx'y'', xx'y''-yy'y''+xy'x''+yx'x''). \end{array}$$

Un calcul semblable montre que

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

D'où $((x,y).(x',y')).(x'',y'') = (x,y).((x',y').(x'',y''))$.

Montrons que la multiplication de $\mathbb{R}^2$ est distributive par rapport à l'addition de $\mathbb{R}^2$. Soient (x,y), (x',y') et (x'',y'') des éléments de $\mathbb{R}^2$. Alors, on a :

$$\begin{array}{rcl} (x,y).((x',y')+(x'',y'')) & = & (x,y).(x'+x'', y'+y'') \\ & = & (xx'+xx''-yy'-yy'', xy'+xy''+yx'+yx'') \\ & = & ((xx'-yy')+(xx''-yy''), (xy'+yx')+(xy''+yx'')) \\ & = & (x,y).(x',y')+(x,y).(x'',y''). \end{array}$$

3. Enfin, pour montrer que $\mathbb{R}^2$ est un corps, il faut montrer que tout élément non nul admet un inverse pour la multiplication. Soit $(x,y) \in \mathbb{R}^2 \setminus \{0\}$ non nul dans $\mathbb{R}^2$. On vérifie facilement que :

$$(x,y).\left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right) = (1,0).$$

Ceci achève la démonstration. ∎

On montre maintenant que le corps $\mathbb{R}$ peut être identifié avec un sous-ensemble de $\mathbb{R}^2$ et ce, de sorte que l'addition et la multiplication de $\mathbb{R}^2$ prolongent celle de $\mathbb{R}$. Attention, par *identifié*, on entend que l'on veut déterminer un sous-ensemble de $\mathbb{R}^2$ qui soit en bijection avec $\mathbb{R}$.

Proposition 1.2 – *L'application*

$$\begin{array}{rccc} \phi & : & \mathbb{R} & \longrightarrow & \mathbb{R}^2 \\ & & a & \mapsto & (a,0) \end{array}$$

est injective. De plus, elle est compatible avec les additions et les multiplications de $\mathbb{R}$ *et* $\mathbb{R}^2$ *au sens où* $\phi(0) = (0,0)$*,* $\phi(1) = (1,0)$ *et, pour tous* $a, b \in \mathbb{R}$*,* $\phi(a+b) = \phi(a) + \phi(b)$ *et* $\phi(ab) = \phi(a)\phi(b)$*.*

Démonstration : C'est une vérification facile dont les détails sont laissés en exercice. ∎

Remarque 1.3 –
1. Soit R le sous-ensemble de $\mathbb{R}^2$ défini par $R = \{(a,0)\ ; a \in \mathbb{R}\}$. Le théorème 1.2 montre que les ensembles $\mathbb{R}$ et R sont en bijection. En effet, R est l'image de ϕ. De plus, il assure que cette bijection respecte les multiplications et additions de $\mathbb{R}$ et $\mathbb{R}^2$ au sens où, pour tous $a, b \in \mathbb{R}$, on a $(a+b,0) = (a,0) + (b,0)$ et $(ab,0) = (a,0)(b,0)$. Attention, dans ces deux dernières équations, la première addition (resp. multiplication) est celle de $\mathbb{R}$ tandis que la seconde est celle de $\mathbb{R}^2$. Ainsi, $\mathbb{R}$ muni de son addition et de sa multiplication, d'une part, et R muni de l'addition et de la multiplication de $\mathbb{R}^2$ se comportent exactement de la même façon.

En conséquence, $\mathbb{R}$ qui n'est pas un sous-ensemble de $\mathbb{R}^2$ à proprement parler, sera tout de même considéré comme sous-ensemble de $\mathbb{R}^2$ et on se permettra d'écrire $\mathbb{R} \subseteq \mathbb{R}^2$.
2. Posons $i = (0,1) \in \mathbb{R}^2$. Un calcul simple montre que, pour tout réel b, $(0,b) = (0,1)(b,0)$, c'est-à-dire que $(0,b) = i(b,0)$. En outre, on a $i^2 = -(1,0)$.
3. La conséquence pratique du point 1 ci-dessus est que, dans la pratique, un nombre réel a sera confondu avec son image $(a,0)$ dans $\mathbb{R}^2$. Pour $a, b \in \mathbb{R}$, on écrira donc

$$(a,b) = (a,0) + (0,b) = (a,0) + (0,1)(b,0) = a + ib.$$

Dans cette dernière équation, la première égalité est justifiée par la défintion de l'addition dans $\mathbb{R}^2$, la seconde a été vue au point 2 ci-dessus et, la troisième est justifiée par le point 1 ci-dessus. Il faut bien prendre garde que cette troisième équation repose sur un abus d'écriture car on y remplace $(a,0)$ par a et $(b,0)$ par b, ce qui rigoureusement parlant n'a pas de sens.

Avec ces notations, on obtient par exemple la relation : $i^2 = -1$.

Définition 1.4 – *L'ensemble* $\mathbb{R}^2$ *muni de l'addition et de la multiplication définies ci-dessus est appelé le corps des nombres complexes et est noté* $\mathbb{C}$*. Les éléments de* $\mathbb{C}$ *sont appelés les nombres complexes.*

Remarque 1.5 –
1. Il résulte de ce qui précède que, pour tout $z \in \mathbb{C}$, il existe un unique couple $(a,b) \in \mathbb{R}^2$ tel que $z = a + ib$.
2. Avec les notations du point 1 ci-dessus, a est appelé la partie réelle de z et b sa partie imaginaire. La partie réelle d'un nombre complexe z sera notée $\mathrm{Re}(z)$ et sa partie imaginaire sera notée $\mathrm{Im}\,(z)$.
3. Les nombres complexes dont la partie réelle est nulle sont appelés des imaginaires purs. Via l'identification décrite ci-dessus, les nombres réels sont donc les nombres complexes dont la partie imaginaire est nulle.
4. Dans la pratique, pour travailler avec $\mathbb{C}$, il suffit de se souvenir des trois propriétés suivantes :
(i) $\mathbb{C}$ est un corps commutatif qui contient $\mathbb{R}$ et dont l'addition et la multiplication prolongent celles de $\mathbb{R}$;

(ii) tout nombre complexe z s'écrit de façon unique $z = a + ib$, où a et b sont des nombres réel (cette écriture sera appelée la forme canonique de z) ;
(iii) $i^2 = -1$.

La remarque suivante est très importante dans la pratique. Elle affirme que $\mathbb{C}$ est un anneau intègre, ce qui se déduit immédiatement du fait que c'est un corps.

Remarque 1.6 – Soient z, z' des nombres complexes. Si $zz' = 0$, alors ou bien $z = 0$ ou bien $z' = 0$. En effet, si l'on suppose que $z \neq 0$, alors ($\mathbb{C}$ étant un corps), il existe un inverse multiplicatif pour z, c'est-à-dire un complexe z'' tel que $z''z = 1$. Mais alors, de $zz' = 0$, on tire que $z' = z''zz' = 1.0 = 0$.

Exercice 1.7 – Montrer que pour tous nombres complexes x, y et tout entier n non nul, on a :
1. $x^n - y^n = (x - y)\sum_{k=0}^{n-1} x^k y^{n-1-k}$,
2. $(x + y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}$.

Proposition 1.8 – *L'ensemble des solutions dans* $\mathbb{C}$ *de l'équation* $z^2 + 1 = 0$ *est* $\{-i, i\}$.

Démonstration : Il est clair que $-i$ et i sont solutions de l'équation $z^2 + 1 = 0$. Réciproquement, soit $z \in \mathbb{C}$ tel que $z^2 + 1 = 0$. On a $z^2 + 1 = z^2 - i^2 = (z - i)(z + i) = 0$. Comme $\mathbb{C}$ est intègre, il s'ensuit que $z \in \{-i, i\}$. ∎

On en vient maintenant à la définition de *conjugué* et de *module* d'un nombre complexe.

Définition 1.9 – *Soit* $z \in \mathbb{C}$ *un nombre complexe de forme canonique* $z = x + iy$ $(x, y \in \mathbb{R})$.
1. On appelle nombre complexe conjugué de z *le nombre complexe, noté* $\overline{z}$, *et défini par* $\overline{z} = x - iy$.
2. On appelle module de z *le nombre réel, noté* $|z|$, *et défini par* $|z| = \sqrt{x^2 + y^2}$

Remarque 1.10 – On a vu plus haut que $\mathbb{R} \subseteq \mathbb{C}$ (après identification adéquate). On a aussi remarqué que l'addition de $\mathbb{C}$ et la multiplication de $\mathbb{C}$ restreintes à $\mathbb{R}$ n'etaient autres que l'addition et la multiplication de $\mathbb{R}$. Il en va de même pour la valeur absolue (définie sur $\mathbb{R}$) et le module (défini sur $\mathbb{C}$) : la restriction à $\mathbb{R}$ du module n'est autre que la valeur absolue.

Proposition 1.11 – *Soient* $z, z' \in \mathbb{C}$. *On a :*
(i) $\overline{z + z'} = \overline{z} + \overline{z'}$, $\overline{zz'} = \overline{z}\,\overline{z'}$ *et, si* $z \neq 0$, $\overline{z^{-1}} = \overline{z}^{-1}$;
(ii) $\mathrm{Re}(z) = \frac{1}{2}(z + \overline{z})$ *et* $\mathrm{Im}\,(z) = \frac{1}{2i}(z - \overline{z})$;
(iii) $|\mathrm{Re}(z)| \leq |z|$ *et* $|\mathrm{Im}\,(z)| \leq |z|$;
(iv) $|z|^2 = z\overline{z}$ *et, si* $z \neq 0$, $z^{-1} = (|z|^2)^{-1}\overline{z}$;
(v) si $|z| = 1$, $z^{-1} = \overline{z}$;
(vi) $|zz'| = |z||z'|$ *et, si* $z' \neq 0$, $|z(z')^{-1}| = |z||z'|^{-1}$;
(vii) pour tout $n \in \mathbb{N}$, $|z^n| = |z|^n$;
(viii) $||z| - |z'|| \leq |z + z'| \leq |z| + |z'|$.

Démonstration : Les points (i) à (vii) sont de simples vérifications. Ils sont donc laissés en exercice. On démontre maintenant le point (viii). On a

$$\begin{aligned} |z+z'|^2 &= (z+z')(\overline{z}+\overline{z'}) \\ &= |z|^2+|z'|^2+(z\overline{z'}+\overline{z}z') \\ &= |z|^2+|z'|^2+2\mathrm{Re}(z\overline{z'}) \\ &\leq |z|^2+|z'|^2+2|z||z'| \\ &= (|z|+|z'|)^2. \end{aligned}$$

Ce dont on déduit que $|z+z'| \leq |z|+|z'|$.

Mais, cette identité étant vraie pour tous complexes z et z', on peut l'appliquer à $z+z'$ et $-z'$, ce qui donne $|z| \leq |z+z'|+|z'|$ et à $z+z'$ et $-z$, ce qui donne $|z'| \leq |z+z'|+|z|$. Finalement, il vient que $-|z+z'| \leq |z|-|z'| \leq |z+z'|$, c'est-à-dire que $||z|-|z'|| \leq |z+z'|$. ∎

2 Nombres complexes et trigonométrie.

On commence par rappeler les propriétés des fonctions sinus et cosinus dont on aura besoin dans la suite. Ces propriétés relèvent d'un cours d'analyse. Elles sont donc admises ici.

Les fonctions

$$\sin : \mathbb{R} \longrightarrow \mathbb{R} \qquad et \qquad \cos : \mathbb{R} \longrightarrow \mathbb{R}$$

vérifient les propriétés suivantes.
1. Les fonctions sinus et cosinus sont 2π-périodique. La fonction cosinus est paire. La fonction sinus est impaire. On a $\cos(0)=1$ et $\sin(0)=0$. Pour tout réel θ, $\cos(\theta)^2+\sin(\theta)^2=1$.
2. Soient x, y des réels tels que $x^2+y^2=1$. Il existe un unique réel $\theta_0 \in [0, 2\pi[$ tel que $x=\cos(\theta_0)$ et $y=\sin(\theta_0)$. De plus, compte tenu de la 2π-périodicité des fonctions sinus et cosinus, $\{\theta \in \mathbb{R} \ ; \ x=\cos(\theta),\ y=\sin(\theta)\} = \{\theta_0+2k\pi \ ; \ k \in \mathbb{Z}\}$.
3. Pour tous $a, b \in \mathbb{R}$, on a :

$$\cos(a+b)=\cos(a)\cos(b)-\sin(a)\sin(b) \qquad \text{et} \qquad \sin(a+b)=\sin(a)\cos(b)+\sin(b)\cos(a).$$

Ces formules sont appelées formules d'addition. Elles se retranscrivent facilement dans $\mathbb{C}$ comme le montre le lemme suivant.

Lemme 2.1 – *Soient $a, b \in \mathbb{R}$. On a dans $\mathbb{C}$ la relation suivante :*

$$\cos(a+b)+i\sin(a+b)=(\cos(a)+i\sin(a))(\cos(b)+i\sin(b)).$$

Démonstration : C'est une conséquence facile des formules d'addition ci-dessus et de l'identité $i^2=-1$. ∎

Proposition 2.2 – **(Formule de Moivre.)**
Soit $\theta \in \mathbb{R}$. Pour tout $n \in \mathbb{Z}$, on a, dans $\mathbb{C}$, l'identité suivante :

$$(\cos(\theta)+i\sin(\theta))^n=\cos(n\theta)+i\sin(n\theta).$$

Démonstration : On commence par montrer que l'équation ci-dessus est vraie pour tout entier naturel. Il est clair que cette identité est vraie pour $n=0$ puisque, par convention, $z^0=1$ pour tout complexe z. Soit à présent $n \in \mathbb{N}$ et supposons que $(\cos(\theta)+i\sin(\theta))^n=\cos(n\theta)+i\sin(n\theta)$.

Alors, compte tenu de lemme 2.1, $(\cos(\theta)+i\sin(\theta))^{n+1} = (\cos(n\theta)+i\sin(n\theta))(\cos(\theta)+i\sin(\theta)) = \cos(n\theta+\theta)+i\sin(n\theta+\theta) = \cos((n+1)\theta)+i\sin((n+1)\theta)$. Il reste donc à montrer que la formule proposée est vraie pour un entier $n < 0$. (Rappelons que, par définition, si n est un entier strictement négatif et z un complexe non nul, $z^n = (z^{-1})^{-n}$.) Ainsi, posons $z = \cos(\theta)+i\sin(\theta)$. Alors, comme z est de module 1, son inverse est son conjugué. On a donc $z^{-1} = \cos(\theta)-i\sin(\theta) = \cos(-\theta)+i\sin(-\theta)$. De plus, comme $-n \geq 0$, en appliquant ce qui précède on obtient que $z^n = (z^{-1})^{-n} = (\cos(-\theta)+i\sin(-\theta))^{-n} = \cos((-n)(-\theta))+i\sin((-n)(-\theta)) = \cos(n\theta)+i\sin(n\theta)$. La démonstration est donc complète. ∎

Application de la formule de Moivre. La formule de Moivre (jointe à la formule du binôme) a une conséquence utile dans la pratique. Étant donné un entier naturel n et un réel θ, elle permet d'exprimer $\cos(n\theta)$ et $\sin(n\theta)$ en fonction de $\cos(\theta)$ et $\sin(\theta)$. On montre ci-dessous sur des exemples simples le procédé qui permet d'obtenir de telles expressions.

Pour $n = 2$,

$$\begin{aligned}\cos(2\theta)+i\sin(2\theta) &= (\cos(\theta)+i\sin(\theta))^2 \\ &= ((\cos(\theta))^2-(\sin(\theta))^2+2i\sin(\theta)\cos(\theta)\end{aligned}.$$

D'où l'on tire que $\cos(2\theta) = (\cos(\theta))^2-(\sin(\theta))^2$ et $\sin(2\theta) = 2\sin(\theta)\cos(\theta)$.

Pour $n = 3$,

$$\begin{aligned}\cos(3\theta)+i\sin(3\theta) &= (\cos(\theta)+i\sin(\theta))^3 \\ &= (\cos(\theta))^3+3i(\cos(\theta))^2\sin(\theta)-3\cos(\theta)(\sin(\theta))^2-i(\sin(\theta))^3\end{aligned}$$

D'où l'on tire que $\cos(3\theta) = 4(\cos(\theta))^3-3\cos(\theta)$ et $\sin(3\theta) = 3\sin(\theta)-4(\sin(\theta))^3$.

Pour $n = 4$,

$$\begin{aligned}\cos(4\theta)+i\sin(4\theta) &= (\cos(\theta)+i\sin(\theta))^4 \\ &= (\cos(\theta))^4+4i(\cos(\theta))^3\sin(\theta)-6(\cos(\theta))^2(\sin(\theta))^2 \\ &\quad -4i\cos(\theta)(\sin(\theta))^3+(\sin(\theta))^4\end{aligned}$$

D'où l'on tire que $\cos(4\theta) = 8(\cos(\theta))^4-8(\cos(\theta))^2+1$, $\sin(4\theta) = \sin(\theta).(8(\cos(\theta))^3-4\cos(\theta))$.

La notation d'Euler. Considérons la fonction suivante :

$$\begin{array}{rcccc} f & : & \mathbb{R} & \longrightarrow & \mathbb{C} \\ & & x & \mapsto & \cos(x)+i\sin(x)\end{array}$$

On peut exprimer les formules d'addition (lemme 2.1) par

$$\text{pour tous} \quad x,y \in \mathbb{R},\ f(x)f(y) = f(x+y).$$

On peut aussi exprimer la formula de Moivre (proposition 2.2) par

$$\text{pour tout} \quad x \in \mathbb{R}, \quad \text{et tout} \quad n \in \mathbb{Z}, \quad f(x)^n = f(nx).$$

Cela suggère immédiatement que les propriétés de f ressemblent beaucoup aux propriétés de la fonction exponentielle. Pour cette raison, Euler a introduit la notation suivante :

$$\text{pour } x \in \mathbb{R},\ e^{ix} = \cos(x)+i\sin(x).$$

On a alors la proposition suivante.

Proposition 2.3 – *Pour $x, y \in \mathbb{R}$ et $n \in \mathbb{Z}$:*
1. $|e^{ix}| = 1$,
2. $e^{ix}e^{iy} = e^{i(x+y)}$,
3. $(e^{ix})^n = e^{inx}$,
4. $\overline{e^{ix}} = (e^{ix})^{-1} = e^{-ix}$,
5. $e^{i.0} = e^0 = 1$, $e^{2n\pi i} = 1$, $e^{i\pi} = -1$,
6. $\cos(x) = \dfrac{1}{2}(e^{ix} + e^{-ix})$ *et* $\sin(x) = \dfrac{1}{2i}(e^{ix} - e^{-ix})$ *(formules d'Euler).*

Démonstration : Les points 1 et 5 découlent facilement de la définition, 2 est une retranscription des formules d'addition, 3 une retranscription de la formule de Moivre et 4 est un cas particulier de la formule de Moivre (avec $n = -1$) puisque $|e^{ix}| = 1$. Enfin, le point 6 se déduit de ce qui précède et du second point de la proposition 1.11. ∎

Les formules de la proposition précédente sont très faciles à retenir. Elles permettent en outre de retrouver des formules beaucoup moins faciles à mémoriser.

Exemple 2.4 – Soient $a, b \in \mathbb{R}$, $\cos(a)\cos(b) = \frac{1}{2}\left(\cos(a+b) + \cos(a-b)\right)$. En effet, on a

$$\begin{aligned}\cos(a)\cos(b) &= \tfrac{1}{2}\left(e^{ia} + e^{-ia}\right)\tfrac{1}{2}\left(e^{ib} + e^{-ib}\right)\\ &= \tfrac{1}{4}\left(e^{i(a+b)} + e^{-i(a+b)} + e^{i(a-b)} + e^{-i(a-b)}\right)\\ &= \tfrac{1}{4}\left(2\cos(a+b) + 2\cos(a-b)\right)\\ &= \tfrac{1}{2}\left(\cos(a+b) + \cos(a-b)\right).\end{aligned}$$

Exercice 2.5 – Soient $a, b \in \mathbb{R}$. Retrouver de manière analogue les formules qui donnent $\sin(a)\sin(b)$.

Exemple 2.6 – Soient $p, q \in \mathbb{R}$. On a

$$\begin{aligned}e^{ip} + e^{iq} &= e^{i\left(\frac{p+q}{2}\right)}.\left(e^{i\left(\frac{p-q}{2}\right)} + e^{i\left(\frac{-p+q}{2}\right)}\right)\\ &= e^{i\left(\frac{p+q}{2}\right)}.2\cos\left(\frac{p-q}{2}\right),\end{aligned}$$

d'où l'on tire que :

$$\begin{cases}\cos p + \cos q = 2\cos\left(\dfrac{p+q}{2}\right).\cos\left(\dfrac{p-q}{2}\right)\\ \sin p + \sin q = 2\sin\left(\dfrac{p+q}{2}\right).\cos\left(\dfrac{p-q}{2}\right).\end{cases}$$

Exercice 2.7 – Soient $p, q \in \mathbb{R}$. Retrouver de manière analogue les formules qui donnent $\cos p - \cos q$ et $\sin p - \sin q$.

Enfin, on peut procéder à des *linéarisations* telles que les suivantes.

Exemple 2.8 – On a, en utilisant la formule du binôme,

$$\cos^2\theta = \frac{1}{4}\left(e^{2i\theta} + e^{-2i\theta} + 2\right),$$

et

$$\sin^3\theta = \left(\frac{-1}{8i}\right)\left(e^{3i\theta} - 3e^{i\theta} + 3e^{-i\theta} - e^{-3i\theta}\right).$$

Il s'ensuit que

$$\begin{aligned}\cos^2\theta.\sin^3\theta &= \left(\frac{-1}{32i}\right)\left((e^{5i\theta} - e^{-5i\theta}) - (e^{3i\theta} - e^{-3i\theta}) - 2(e^{i\theta} - e^{-i\theta})\right)\\ &= \left(\frac{-1}{32i}\right)(2i\sin 5\theta - 2i\sin 3\theta - 4i\sin\theta)\\ &= -\frac{1}{16}\sin 5\theta + \frac{1}{16}\sin 3\theta + \frac{1}{8}\sin\theta.\end{aligned}$$

Exercice 2.9 – Linéariser de manière analogue $\cos^6\theta$.

On termine cette section par un point très important qui découle de ce qui précède concernant le lien entre nombres complexes et trigonométrie. Il s'agit de montrer que tout nombre complexe peut être exprimé sous une forme dite *forme trigonométrique*.

On commence par une remarque facile sur les nombres complexes de module 1.

Remarque 2.10 – Soit z un nombre complexe de module 1. Si x et y sont respectivement les parties réelles et imaginaires de z, on a $z = x + iy$ et $x^2 + y^2 = 1$. Compte tenu des rappels fait en début de section sur les fonctions sinus et cosinus, il existe un réel θ tel que $x = \cos(\theta)$ et $y = \sin(\theta)$. On a donc alors :

$$z = \cos(\theta) + i\sin(\theta).$$

Soit maintenant z un nombre complexe non nul quelconque, de partie réelle x et de partie imaginaire y, de sorte que $z = x+iy$. Comme z est non nul, $|z|$ n'est pas nul et on peut considérer le nombre complexe $z/|z|$ qui, lui, est de module 1. Par suite, il existe $\theta \in \mathbb{R}$ tel que

$$\frac{z}{|z|} = \cos(\theta) + i\sin(\theta),$$

ce qui se réécrit encore

$$z = |z|\,(\cos(\theta) + i\sin(\theta)) = |z|e^{i\theta}.$$

Dans la pratique, écrire un nombre complexe non nul sous la forme du produit d'un nombre réel strictement positif et d'une exponentielle complexe est souvent très utile. C'est pourquoi l'on veut étudier en détail cette possibilité.

Commençons par donner un nom à une telle écriture. Si z est un nombre complexe non nul, une écriture sous forme trigonométrique de z est une expression

$$z = re^{i\theta},$$

où r est un réel strictement positif et θ un réel quelconque. Ce qui précède montre que tout nombre complexe non nul admet une écriture sous forme trigonométrique. Le théorème suivant montre qu'un telle écriture n'est pas (tout-à-fait) unique.

Théorème 2.11 – *Si r, r' sont des réels strictement positifs et θ, θ' des réels, alors les assertions suivantes sont équivalentes :*
(i) $re^{i\theta} = r'e^{i\theta'}$;
(ii) $r = r'$ et il existe $k \in \mathbb{Z}$ tel que $\theta' - \theta = 2k\pi$.

Démonstration : Montrons que (ii) entraîne (i). On suppose donc que $r = r'$ et qu'il existe $k \in \mathbb{Z}$ tel que $\theta' - \theta = 2k\pi$. On a alors $r'e^{i\theta'} = re^{i(\theta+2k\pi)} = re^{i\theta}e^{i2k\pi} = re^{i\theta}$.
Montrons maintenant que (i) entraîne (ii). On suppose donc que $re^{i\theta} = r'e^{i\theta'}$. En prennant le module de chacun des termes de cette égalité, on obtient donc que $|re^{i\theta}| = |r'e^{i\theta'}|$, c'est-à-dire que $|r||e^{i\theta}| = |r'||e^{i\theta'}|$, et compte tenu du premier point de la proposition 2.3, il s'ensuit que $r = |r| = |r'| = r'$. On a donc $e^{i\theta} = e^{i\theta'}$. En appliquant à nouveau la proposition 2.3, il s'ensuit que $e^{i\theta'}e^{-i\theta} = 1$, c'est-à-dire que $e^{i(\theta'-\theta)} = 1$. Cela signifie que

$$\cos(\theta' - \theta) = 1 \quad \text{et} \quad \sin(\theta' - \theta) = 0.$$

En utilisant les propriétés, rappelées en début de section, des fonctions sinus et cosinus, il s'ensuit qu'il existe $k \in \mathbb{Z}$ tel que $\theta' - \theta = 2k\pi$. ∎

Remarque 2.12 – Soit z un nombre complexe non nul. Ce qui précède montre que, si r est un réel strictement positif et θ un réel tels que $z = re^{i\theta}$, alors :
1. $r = |z|$;
2. l'ensemble des réels θ' tels que $z = re^{i\theta'}$ est

$$\{\theta + 2k\pi \ ; \ k \in \mathbb{Z}\}.$$

Définition 2.13 – *Soit z un nombre complexe non nul. Tout réel θ tel que $z = |z|e^{i\theta}$ s'appelle un argument de z.*

Exemple 2.14 – On montre facilement que les arguments de 1 sont les réels $2k\pi$, $k \in \mathbb{Z}$. En particulier, 0 est un argument de 1.

Proposition 2.15 – *Soient z et z' deux complexes non nuls. Soient θ un argument de z et θ' un argument de z'. Soit $n \in \mathbb{Z}$. Alors :*
1. $\theta + \theta'$ est un argument de zz' ;
2. $-\theta$ est un argument de $1/z$;
3. $n\theta$ est un argument de z^n.

Démonstration : La démonstration est laissée en exercice. Pour le troisième point, on conseille de montrer le résultat pour $n \in \mathbb{N}$ dans un premier temps, puis d'utiliser le second point pour l'étendre à tout entier. ∎

Exercice 2.16 – *Soit z un nombre complexe non nul et θ un argument de z. Alors* $\mathrm{Re}(z) = |z|\cos(\theta)$ *et* $\mathrm{Im}\,(z) = |z|\sin(\theta)$.

3 Équations polynomiales et nombres complexes.

Etant donné un anneau A, par exemple $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, résoudre dans A l'équation polynomiale de degré d ($d \in \mathbb{N}$) et de coefficients $a_0, \ldots, a_d \in A$, avec $a_d \neq 0$, notée (un peu abusivement)

$$a_n x^n + \ldots + a_2 x^2 + a_1 x + a_0 = 0,$$

c'est chercher tous les éléments $a \in A$ tels que

$$a_n a^n + \ldots + a_2 a^2 + a_1 a + a_0 = 0.$$

Comme il est bien connu, le défaut majeur de $\mathbb{R}$ est qu'il existe des équations à coefficients réels qui n'ont aucune solution dans $\mathbb{R}$. C'est par exemple le cas de l'équation $x^2+1=0$. Mais, si l'équation $x^2+1=0$ est considérée comme une équation dans $\mathbb{C}$, alors elle admet des solutions, à savoir i et $-i$ (et en fait aucune autre).

Historiquement, la raison de l'introduction du corps des nombres complexes est précisément de trouver un corps contenant $\mathbb{R}$ et dans lequel toute équation polynomiale admet au moins une solution. A ce sujet, voir le théorème de d'Alembert (cf théorème 3.3.1).

3.1 Equations du second degré.

Dans cette sous-section, on s'intéresse aux équations du second degré dans $\mathbb{C}$. Se donner une telle équation revient à se donner trois complexes a, b, c avec $a \neq 0$. L'équation s'écrit alors :

$$ax^2 + bx + c = 0.$$

Un cas particulier (dont on va bientôt voir qu'il est crucial) est celui où $a = 1$, $b = 0$ et c est quelconque. Dans ce cas, l'équation à résoudre est $x^2 + c = 0$, où encore $x^2 = -c$. En d'autre termes, résoudre cette équation revient à chercher les racines carrées de $-c$.

Racines carrées d'un nombre complexe. Le lemme suivant montre que tout nombre complexe admet une racine carrée. Il précise en fait que tout nombre complexe non nul admet exactement deux racines carrées distinctes.

Lemme 3.1.1 – *Soit z_0 un nombre complexe et $E = \{z \in \mathbb{C}\,;\, z^2 = z_0\}$ l'ensemble de ses racines carrées.*
1. Si $z_0 = 0$, on a $E = \{0\}$.
2. Si $z_0 \neq 0$, et si $\theta \in \mathbb{R}$ est un argument de z_0 (de sorte que $z_0 = |z_0|e^{i\theta}$), alors $E = \{\sqrt{|z_0|}e^{i\theta/2}, -\sqrt{|z_0|}e^{i\theta/2}\}$ et les deux éléments de cet ensemble sont distincts.

Démonstration : Le premier point est évident. Supposons donc que z_0 est non nul. Il peut alors être écrit sous forme trigonométrique et, si θ est un argument de z_0, on a $z_0 = |z_0|e^{i\theta}$. Remarquons alors que $z_0 = (\sqrt{|z_0|}e^{i\theta/2})^2$. Ainsi, pour tout $z \in \mathbb{C}$, on a

$$\begin{array}{ll} & z^2 = z_0 \\ \text{ssi} & z^2 = (\sqrt{|z_0|}e^{i\theta/2})^2 \\ \text{ssi} & z^2 - (\sqrt{|z_0|}e^{i\theta/2})^2 = 0 \\ \text{ssi} & (z - \sqrt{|z_0|}e^{i\theta/2})(z + \sqrt{|z_0|}e^{i\theta/2}) = 0. \end{array}$$

Comme $\mathbb{C}$ est intègre, il s'ensuit que $E = \{\sqrt{|z_0|}e^{i\theta/2}, -\sqrt{|z_0|}e^{i\theta/2}\}$. Enfin, si l'on suppose que $\sqrt{|z_0|}e^{i\theta/2} = -\sqrt{|z_0|}e^{i\theta/2}\}$, il vient que $e^{i\theta/2} = 0$, ce qui est absurde puisque $e^{i\theta/2}$ est de module 1. Donc, les deux éléments de E sont distincts. ∎

Remarque 3.1.2 – Le lemme 3.1.1 montre que tout complexe non nul admet deux racines carrées distinctes et que, si δ est l'une d'entre elle, l'autre est $-\delta$.

Le lemme 3.1.1 est très important en ce qu'il répond à la question de savoir si, étant donné un nombre complexe, il existe des racines carrées pour ce nombre et le cas échéant, combien. Il présente cependant un défaut pratique. En effet, étant donné un nombre complexe non nul, il est souvent impossible de déterminer un argument pour ce nombre complexe. La détermination

explicite de ses racines carrées par le biais du théorème ci-dessus est donc mise en échec.

Voici donc une autre approche qui, elle, utilise la description des complexes sous forme algébrique.

Soit z_0 un nombre complexe non nul et soient $\alpha, \beta \in \mathbb{R}$ tels que $z_0 = \alpha + i\beta$. On veut exprimer les racines carrées de z_0 en fonction de α et β.

Si $\beta = 0$, deux cas se présentent suivant le signe du réel α. Si $\alpha > 0$, les racines carrées de z_0 sont $\sqrt{\alpha}$ et $-\sqrt{\alpha}$. Si $\alpha < 0$, les racines carrées de z_0 sont $i\sqrt{-\alpha}$ et $-i\sqrt{-\alpha}$.

Supposons maintenant $\beta \neq 0$. Soit $z = x + iy$ une solution de $z^2 = z_0$. On a donc

$$\begin{cases} x^2 + y^2 = \sqrt{\alpha^2 + \beta^2} \\ x^2 - y^2 = \alpha \\ 2xy = \beta. \end{cases}$$

Par conséquent,

$$x^2 = \frac{1}{2}\left(\sqrt{\alpha^2 + \beta^2} + \alpha\right),\ y^2 = \frac{1}{2}\left(\sqrt{\alpha^2 + \beta^2} - \alpha\right),$$

et on en déduit x et y sachant que xy est du signe de β. On trouve alors deux valeurs possibles pour z. Ce sont les racines carrées de a, puisque le lemme 3.1.1 assure que a a exactement deux racines carrées.

Exemple 3.1.3 – Déterminons les racines carrées de $z_0 = 2+i$. Comme la forme trigonométrique de z_0 n'a pas d'argument remarquable, on va calculer les racines carrées z de z_0 sous la forme algébrique $z = x + iy$. La relation $z^2 = 2 + i$ donne le système

$$\begin{cases} x^2 + y^2 = \sqrt{5} \\ x^2 - y^2 = 2 \\ 2xy = 1. \end{cases}$$

On en tire $x^2 = \frac{\sqrt{5}+2}{2}$, $y^2 = \frac{\sqrt{5}-2}{2}$. Comme $xy > 0$ par la dernière égalité du système, on obtient que les racines carrées de $2 + i$ sont

$$\sqrt{\frac{\sqrt{5}+2}{2}} + i\sqrt{\frac{\sqrt{5}-2}{2}} \quad \text{et} \quad -\sqrt{\frac{\sqrt{5}+2}{2}} - i\sqrt{\frac{\sqrt{5}-2}{2}}.$$

Équation du second degré générale. On en vient maintenant à l'équation du second degré en toute généralité. Sa résolution repose sur le théorème suivant.

Théorème 3.1.4 – *Soient a, b, c des nombres complexes avec a non nul. On pose $\Delta = b^2 - 4ac$ et on note δ une racine carrée (arbitraire) de Δ.*
1. L'ensemble $\mathcal{S}$ des solutions complexes de l'équation $az^2 + bz + c = 0$ est :

$$\mathcal{S} = \left\{\frac{-b+\delta}{2a},\ \frac{-b-\delta}{2a}\right\}.$$

2. Les solutions $z_1 = \dfrac{-b+\delta}{2a}$ et $z_2 = \dfrac{-b-\delta}{2a}$ sont distinctes si et seulement si $\Delta \neq 0$.
3. Pour tout nombre complexe z, on a $az^2 + bz + c = a(z - z_1)(z - z_2)$.

Démonstration : Etant donnés les complexes a, b et c avec a non nul, posons $\Delta = b^2 - 4ac$ et considérons une racine carrée δ arbitraire de Δ (existence assurée par le lemme 3.1.1). Enfin, posons

$$z_1 = \frac{-b+\delta}{2a} \quad \text{et} \quad z_2 = \frac{-b-\delta}{2a}$$

Pour tout nombre complexe z, on a :

$$\begin{aligned} az^2+bz+c &= a\left(z^2+\frac{b}{a}z+\frac{c}{a}\right) \\ &= a\left((z+\frac{b}{2a})^2-\frac{b^2}{4a^2}+\frac{c}{a}\right) \\ &= a\left((z+\frac{b}{2a})^2-\frac{\Delta}{4a^2}\right) \\ &= a\left((z+\frac{b}{2a})^2-\frac{\delta^2}{4a^2}\right) \\ &= a\left(z+\frac{b-\delta}{2a}\right)\left(z+\frac{b+\delta}{2a}\right) \\ &= a(z-z_1)(z-z_2). \end{aligned}$$

Ceci prouve le point 3. Compte tenu de l'intégrité de $\mathbb{C}$, le point 1 s'en déduit immédiatement. Enfin, il est clair que $z_1 = z_2$ si et seulement si $\delta = 0$ c'est-à-dire si et seulement si $\Delta = 0$. ∎

Remarque 3.1.5 – On reprend les notations du théorème 3.1.4.
1. Le nombre complexe Δ s'appelle le discriminant de l'équation $az^2+bz+c=0$. Cette équation admet donc deux solutions distinctes si et seulement si son discriminant est non nul et, si il est nul, elle admet une unique solution.
2. On a les formules suivantes donnant la somme et le produit des solutions de l'équation considérée :

$$z_1+z_2 = -\frac{b}{a}, \quad z_1 z_2 = \frac{c}{a}.$$

3. Supposons que a, b et c sont des nombres réels. Alors, trois cas sont possibles :
(i) si $\Delta > 0$, alors $\delta \in \mathbb{R}$ et z_1 et z_2 sont des nombres réels distincts ;
(ii) si $\Delta = 0$, alors $\delta = 0$ et $z_1 = z_2$ est un nombre réel ;
(iii) si $\Delta < 0$, alors on peut prendre $\delta = i\sqrt{-\Delta}$ qui est donc un imaginaire pur et z_1 et z_2 sont des nombres complexes distincts et conjugués l'un de l'autre.

3.2 Racines n-ièmes d'un nombre complexe.

On en vient maintenant à la résolution d'une équation du type $z^n = a$, où n est un entier naturel non nul fixé et a un nombre complexe fixé. Notons que le cas où $n = 1$ est trivial et que le cas où $n = 2$ a déjà été traité à la sous-section précédente.

Remarquons aussi que résoudre l'équation ci-dessus consiste à déterminer les racines n-ièmes du nombre complexe a.

Il s'avère qu'on peut résoudre ce problème de façon très satisfaisante et que, comme dans le cas des racines carrées, la clé et d'utiliser la forme trigonométrique des nombres complexes.

Racines n-ièmes de l'unité. Il s'avère que la résolution du problème posé ci-dessus passe, en premier lieu, par la détermination des racines n-ièmes de 1. On commence donc par traiter ce problème.

Théorème 3.2.1 – *Soit $n \in \mathbb{N}$, $n \neq 0$. L'ensemble des nombres complexes z tels que $z^n = 1$ est l'ensemble*

$$\{e^{\frac{2ik\pi}{n}} \ ; \ k = 0, 1, \ldots, n-1\}.$$

Cet ensemble est de cardinal n.

Démonstration : Soit z un nombre complexe tel que $z^n = 1$. Comme $|z|^n = 1$, on doit avoir $|z| = 1$. Il existe donc un réel θ tel que $z = e^{i\theta}$. De $z^n = 1$ on tire alors que $e^{in\theta} = 1e^{i.0}$ ce qui entraîne qu'il existe $m \in \mathbb{Z}$ tel que $n\theta = 2m\pi$. La division euclidienne de m par n assure qu'il existe $q \in \mathbb{Z}$ et $k \in \{0, 1, \ldots, n-1\}$ tels que $m = qn+k$. On a alors $n\theta = 2(qn+k)\pi = qn2\pi+2k\pi$. Il s'ensuit que

$$z = e^{i\theta} = e^{i(q2\pi+\frac{2k\pi}{n})} = e^{iq2\pi}e^{i\frac{2k\pi}{n}} = e^{i\frac{2k\pi}{n}}.$$

On a donc montré que tout complexe z tel que $z^n = 1$ est dans l'ensemble $\{e^{\frac{2ik\pi}{n}} \ ; \ k = 0, 1, \ldots, n-1\}$. Réciproquement, si k est un entier tel que $0 \leq k \leq n-1$, on a $(e^{\frac{2ik\pi}{n}})^n = e^{2ik\pi} = 1$. Finalement, on a montré que l'ensemble des complexes z tels que $z^n = 1$ est bien $\{e^{\frac{2ik\pi}{n}} \ ; \ k = 0, 1, \ldots, n-1\}$.

Il reste à prouver que cet ensemble a exactement n éléments. Autrement dit, que les nombres $e^{\frac{2k\pi i}{n}}$, $k = 0, 1, \ldots, n-1$, sont distincts deux-à-deux. Soient k et l des entiers tels que $0 \leq k \leq l \leq n-1$. Supposons $e^{\frac{2k\pi i}{n}} = e^{\frac{2l\pi i}{n}}$. Alors, il existe $p \in \mathbb{Z}$ tel que $k - l = pn$. Mais, comme $0 \leq k \leq l \leq n-1$, cela force à avoir $k = l$. ∎

Remarque 3.2.2 – Soit $n \in \mathbb{N}$, $n \neq 0$. Posons $z_1 = e^{\frac{2i\pi}{n}}$. On déduit immédiatement du théorème 3.2.1 que la liste exhaustive et sans répétition des nombres complexes z tels que $z^n = 1$ est :

$$z_1, z_1^2, \ldots, z_1^{n-1}, z_1^n = 1.$$

Exemple 3.2.3 – Examinons quelques exemples pour des petites valeurs de n.
1. Les complexes z tels que $z^2 = 1$ sont donc

$$e^0 = 1 \quad \text{et} \quad e^{i\pi} = -1.$$

2. Les complexes z tels que $z^3 = 1$ sont donc

$$e^0 = 1, \ j := e^{\frac{2i\pi}{3}} \quad \text{et} \quad j^2 = e^{\frac{4i\pi}{3}}.$$

3. Les complexes z tels que $z^4 = 1$ sont donc

$$e^0 = 1, \ e^{\frac{2i\pi}{4}} = i, \ e^{\frac{4i\pi}{4}} = -1 \quad \text{et} \quad e^{\frac{6i\pi}{4}} = -i.$$

4. Les complexes z tels que $z^5 = 1$ sont donc

$$e^0 = 1, \ e^{\frac{2i\pi}{5}}, \ e^{\frac{4i\pi}{5}} = \left(e^{\frac{2i\pi}{5}}\right)^2, \ e^{\frac{6i\pi}{5}} = \left(e^{\frac{2i\pi}{5}}\right)^3 \quad \text{et} \quad e^{\frac{8i\pi}{5}} = \left(e^{\frac{2i\pi}{5}}\right)^4.$$

Exercice 3.2.4 – Vérifier que

$$e^{\frac{2\pi i}{5}} = \frac{\sqrt{5}-1}{4} + \frac{i\sqrt{10+2\sqrt{5}}}{4}.$$

Remarque 3.2.5 – Les cas traités à l'exemple 3.2.3 ainsi que le résultat de l'exercice 3.2.4 pourraient laisser à penser que pour toute valeur de n on peut trouver une expression algébrique simple des racines n-ièmes de l'unité. Par exemple à partir d'entiers, des quatre opérations usuelles et de l'extraction de racines carrées des nombres réels positifs. En fait, il n'en est rien (sauf dans de rares exceptions). Par exemple, on peut montrer (au prix d'une approche qui relève de la quatrième année) qu'il n'existe pas de telles formules pour $n = 7$.

On termine l'étude des racines n-ièmes de l'unité avec un résultat remarquable, très utile et très simple à démontrer.

Il repose sur une identié remarquable que l'on rappelle maintenant.

Soit z un nombre complexe quelconque et n un entier naturel non nul. On a

$$(1-z)(1+z+\ldots+z^{n-1}) = 1-z^n.$$

La démonstration de ce résultat est laissée en exercice, elle ne pose pas de difficulté.

Proposition 3.2.6 – *Soit n un entier naturel tel que $n \geq 2$. La somme des n racines n-ièmes de l'unité est nulle.*

Démonstration : Soit n un entier naturel non nul, $n \geq 2$. D'après la remarque 3.2.2, si l'on pose $z_1 = e^{\frac{2i\pi}{n}}$, la liste exhaustive et sans répétition des n racines n-ièmes de l'unité est : $z_1, z_1^2, \ldots, z_1^{n-1}, z_1^n = 1$. La somme des n racines n-ièmes de l'unité s'écrit donc : $1 + z_1 + z_1^2 + \ldots + z_1^{n-1}$. Or, l'identité rappelée ci-dessus assure que

$$(1-z_1)(1+z_1+z_1^2+\ldots+z_1^{n-1}) = 1-z_1^n = 0.$$

Comme $z_1 \neq 1$ (puisque $n \neq 1$), il s'ensuit que

$$1+z_1+z_1^2+\ldots+z_1^{n-1} = 1-z_1^n = 0.$$

Le résultat est démontré. ∎

Racines n-ièmes d'un nombre complexe quelconque. On est maintenant en position de déterminer l'ensemble des racines n-ièmes d'un nombre complexe a quelconque. Comme il est clair que 0 admet 0 pour seule racine n-ième, on suppose désormais que a est non nul.

Théorème 3.2.7 – *Soient n un entier naturel non nul et a un nombre complexe non nul.*
1. L'ensemble des nombres complexes z tels que $z^n = a$ est de cardinal n.
2. Si z_0 est un nombre complexe tel que $z_0^n = a$, alors l'ensemble des nombres complexes z tels que $z^n = a$ est

$$\{z_0.e^{\frac{2k\pi i}{n}};\ k = 0,\ 1,\ \ldots, n-1\}.$$

3. Soit θ un argument de a. Si l'on pose $\zeta = |a|^{1/n}e^{\frac{i\theta}{n}}$, on a $\zeta^n = a$.

Démonstration : Posons $\zeta = |a|^{1/n}e^{\frac{i\theta}{n}}$. Il est clair que $\zeta^n = a$, ce qui établit le troisième point. Considérons maintenant un complexe z_0 tel que $z_0^n = a$. (Il en existe un, par exemple ζ.) Pour tout nombre complexe z, $z^n = a$ si et seulement si $z^n = z_0^n$, si et seulement si $(z/z_0)^n = 1$. Le reste de l'énoncé se déduit donc immédiatement du théorème 3.2.1. ∎

Remarque 3.2.8 – Soit n un entier naturel non nul. Soient a un nombre complexe non nul et θ un argument de a. On déduit immédiatement du théorème 3.2.7 que l'ensemble des racines n-ièmes complexes de a est

$$\{|a|^{1/n}e^{i(\frac{\theta+2k\pi}{n})};\ k = 0,\ 1,\ \ldots, n-1\}.$$

3.3 Le théorème de d'Alembert.

On termine cette section sur les équations polynomiales dans $\mathbb{C}$ par un théorème de la plus grande importance. Néanmoins, sa démonstration étant assez délicate, on admet donc ce résultat. Il est connu sous le nom de théorème de d'Alembert.

Théorème 3.3.1 – *Toute équation polynomiale complexe de degré non nul admet une solution dans* $\mathbb{C}$.

Bien sur, ce théorème doit être mis en contraste avec le cas des équation polynomiales réelles qui peuvent fort bien n'admettre aucune solution dans $\mathbb{R}$.

4 *Exercices.*

Exercice 4.1 – Mettre sous la forme $a+bi$ $(a,b\in\mathbb{R})$ les nombres complexes $(5+3i)^{-1}$, $(1+2i)(2-3i)(2+i)(3-2i)$, $(4-3i)(2+3i)(5-3i)^{-1}$, $(4+2i)^{-1}(3-i)^{-1}$.

Exercice 4.2 – Trouver les nombres complexes z solutions de $4z^2+8|z|^2-3=0$ (resp. $|1+z|=1+|z|$).

Exercice 4.3 – Calculer $(1+i)^n+(1-i)^n$ et $(1+i)^n-(1-i)^n$ (penser à la forme trigonométrique).

Exercice 4.4 – Ecrire sous forme trigonométrique les nombres complexes $(1+i\sqrt{3})(\sqrt{3}+i)^{-1}$, $(1+i\tan(\alpha))(1-i\tan(\alpha))^{-1}$, $(1-\cos(\alpha)+i\sin(\alpha))(1+\cos(\alpha)-i\sin(\alpha))^{-1}$.

Exercice 4.5 – Déterminer les entiers n tels que $(1+i\sqrt{3})^n$ soit un nombre réel négatif.

Exercice 4.6 – Montrer que tout nombre complexe de module 1, distinct de -1, peut s'écrire d'une façon et d'une seule sous la forme $\dfrac{1-ia}{1+ia}$, $a\in\mathbb{R}$.

Exercice 4.7 – Trouver x et y réels tels que $\left(\dfrac{1+i}{1+i\sqrt{3}}\right)^{266}=x+iy$.

Exercice 4.8 – Montrer que si $|z|=|z'|=1$ et $zz'\neq -1$ alors $\dfrac{z+z'}{1+zz'}$ est réel.

Exercice 4.9 – Calculer les racines carrées de $8-6i$, $1+4\sqrt{5}i$, $9+40i$, $1+4i\sqrt{3}$.

Exercice 4.10 – Calculer les racines cubiques de $i-\sqrt{3}$.

Exercice 4.11 – Soit $n\in\mathbb{N}^*$. Quelles sont les solutions $z\in\mathbb{C}$ de $(z+i)^n=(z-i)^n$?

Exercice 4.12 – Soit x un nombre complexe non nul. Montrer que si $x+\dfrac{1}{x}=2\cos(\alpha)$ alors pour tout $n\in\mathbb{N}$: $x^n+\dfrac{1}{x^n}=2\cos(n\alpha)$.

Exercice 4.13 – Résoudre dans $\mathbb{C}$ les équations suivantes :
(a) $\overline{z}^3=z$;
(b) $(1-i)z^2-(6-4i)z+(9-7i)=0$;
(c) $z^2-2z(\cos(\varphi))+1=0$;
(d) $\left(\dfrac{z+i}{z-i}\right)^3+\left(\dfrac{z+i}{z-i}\right)^2+\left(\dfrac{z+i}{z-i}\right)+1=0$.

Exercice 4.14 – Déterminer l'ensemble $S = \{z \in \mathbb{C} \; ; \; |z+1| \leq 1 \quad \text{et} \quad |z-1| \leq 1\}$.

Exercice 4.15 – En utilisant les racines 5-ièmes de l'unité, calculez $\cos\left(\frac{2\pi}{5}\right)$, $\sin\left(\frac{2\pi}{5}\right)$.

Exercice 4.16 – Calculez $\cos(5x)$ à l'aide de $\cos(x)$, $\sin(5x)$ à l'aide de $\sin(x)$. Déterminer les valeurs de $\cos\left(\frac{\pi}{10}\right)$, $\sin\left(\frac{\pi}{5}\right)$.

Exercice 4.17 – On sait que la somme des racines n-ièmes de l'unité ($n \geq 2$) est nulle. En partant de cela, calculez :

1. $A := \cos\left(\frac{\pi}{11}\right) + \cos\left(\frac{3\pi}{11}\right) + \cos\left(\frac{5\pi}{11}\right) + \cos\left(\frac{7\pi}{11}\right) + \cos\left(\frac{9\pi}{11}\right)$,
2. $B := \cos\left(\frac{\pi}{7}\right) - \cos\left(\frac{2\pi}{7}\right) + \cos\left(\frac{3\pi}{7}\right)$.

Exercice 4.18 – Soit $n \in \mathbb{N}$; en utilisant $(1+i)^n$ montrez que :

$$\binom{n}{1} - \binom{n}{3} + \binom{n}{5} - \binom{n}{7} + \ldots = 2^{n/2} \sin\frac{n\pi}{4},$$

$$\binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \binom{n}{6} + \ldots = 2^{n/2} \cos\frac{n\pi}{4}.$$

Préciser ce que signifient les ... !

Exercice 4.19 – Etablir les identités suivantes (et précisez dans quoi x varie) :

1. $x^{2p} - 1 = (x^2-1) \prod_{k=1}^{p-1} \left(x^2 - 2x\cos\frac{2k\pi}{2p} + 1\right)$ pour $p \in \mathbb{N}$, $p \geq 2$;
2. $x^{2p+1} - 1 = (x-1) \prod_{k=1}^{p} \left(x^2 - 2x\cos\frac{2k\pi}{2p+1} + 1\right)$ pour $p \in \mathbb{N}$, $p \geq 1$.

Dans chaque cas on introduira les racines n-ièmes de l'unité ($n = 2p$ ou $n = 2p+1$) et on écrira $x^n - 1$ à l'aide de ces racines.

Exercice 4.20 – Démontrez que pour tous les réels φ, h (avec $\sin\frac{h}{2} \neq 0$) on a pour tout $n \in \mathbb{N}^*$:

1. $\sin(\varphi) + \sin(\varphi+h) + \sin(\varphi+2h) + \ldots + \sin(\varphi+nh) = \frac{\sin((n+1)h/2).\sin(\varphi+(nh/2))}{\sin(h/2)}$;
2. $\cos(\varphi) + \cos(\varphi+h) + \cos(\varphi+2h) + \ldots + \cos(\varphi+nh) = \frac{\sin((n+1)h/2).\cos(\varphi+(nh/2))}{\sin(h/2)}$.

Partie V

Polynômes.

Dans ce chapitre, on définit l'anneau des polynômes en une indéterminée à coefficients dans un corps $\mathbb{K}$ commutatif. Les anneaux de polynômes ont des propriétés arithmétiques (c'est-à-dire liées à la divisibilité) très intéressantes. L'étude de ces propriétés est l'objet de la seconde partie. Dans la troisième, on aborde la notion de fonction polynomiale.

1 L'anneau des polynômes à coefficients dans un corps.

Dans toute cette section, sauf mention expresse du contraire, $\mathbb{K}$ est un corps commutatif. L'objectif qui nous guide est de définir la notion de *polynôme à coefficients dans* $\mathbb{K}$.

Définition 1.1 – *On appelle polynôme à coefficients dans* $\mathbb{K}$ *une suite* $(a_i)_{i\in\mathbb{N}} = (a_0, a_1, a_2, \ldots)$ *d'éléments de* $\mathbb{K}$ *n'ayant qu'un nombre fini de termes non nuls. On appelle polynôme nul la suite, notée* 0*, dont tous les termes sont nuls. Soit* $P = (a_i)_{i\in\mathbb{N}}$ *un polynôme ; si* $P \neq 0$*, le plus grand entier* d *tel que* $a_d \neq 0$ *est appelé le degré de* P *et est noté* $\deg P$*. Par convention, le degré du polynôme nul est* $-\infty$*. L'ensemble des polynômes à coefficients dans* $\mathbb{K}$ *est noté* $\mathbb{K}^{(\mathbb{N})}$*.*

On appelle monôme un polynôme $P = (a_0, a_1, a_2, \ldots)$ *dont un terme et un seul est non nul, c'est-à-dire vérifiant la propriété :* $\exists!\, i \in \mathbb{N}$ *tel que* $a_i \neq 0$*.*

On munit l'ensemble $\mathbb{K}^{(\mathbb{N})}$ des polynômes à coefficients dans $\mathbb{K}$ de deux lois de composition interne, une addition et une multiplication, définies de la manière suivante. Étant donnés deux polynômes $P = (a_i)_{i\in\mathbb{N}}$ et $Q = (b_i)_{i\in\mathbb{N}}$, la somme de P et Q est définie par

$$P + Q = (a_i + b_i)_{i\in\mathbb{N}}$$

et le produit de P et Q est défini par

$$PQ = (c_i)_{i\in\mathbb{N}}, \text{ avec } c_i = \sum_{p+q=i} a_p b_q, \text{ pour } i \in \mathbb{N}.$$

Il est clair que la somme de P et Q est bien une suite qui n'a qu'un nombre fini de termes non nuls : si d est le degré de P et e celui de Q, tous les termes de $a_i + b_i$ sont nuls lorsque $i > \sup\{d, e\}$. Il n'est pas non plus très difficile de montrer que le produit PQ est bien une suite qui n'a qu'un nombre fini de termes non nuls. En effet, si $i > d + e$, on a $c_i = \sum_{p+q=i} a_p b_q = 0$ puisque pour que deux entiers p et q soient tels que $p + q > d + e$, il est nécessaire que $p > d$ ou $q > e$. Ainsi, les suites $P + Q$ et PQ ainsi définies sont bien dans $\mathbb{K}^{(\mathbb{N})}$ et on a défini deux lois de composition interne sur $\mathbb{K}^{(\mathbb{N})}$, respectivement appelées addition et multiplication :

$$\begin{array}{rccccc} + & : & \mathbb{K}^{(\mathbb{N})} \times \mathbb{K}^{(\mathbb{N})} & \longrightarrow & \mathbb{K}^{(\mathbb{N})} \\ & & (P, Q) & \mapsto & P + Q \end{array} \qquad \begin{array}{rccccc} \times & : & \mathbb{K}^{(\mathbb{N})} \times \mathbb{K}^{(\mathbb{N})} & \longrightarrow & \mathbb{K}^{(\mathbb{N})} \\ & & (P, Q) & \mapsto & PQ \end{array}.$$

Théorème 1.2 – **Structure de** $(\mathbb{K}^{(\mathbb{N})}, +, \times)$**.** *Muni des lois d'addition et de multiplication définies ci-dessus, l'ensemble* $\mathbb{K}^{(\mathbb{N})}$ *des polynômes à coefficients dans* $\mathbb{K}$ *est un anneau commutatif. L'élément neutre de l'addition est le polynôme nul ; l'élément neutre de la multiplication est le polynôme* $(a_i)_{i\in\mathbb{N}}$ *tel que* $a_0 = 1$ *et* $a_i = 0$*, pour* $i > 0$*.*

Démonstration : Exercice. ∎

Pour faciliter les calculs dans $\mathbb{K}^{(\mathbb{N})}$ et se rapprocher d'avantage de l'intuition, on va donner maintenant une nouvelle description de l'anneau $(\mathbb{K}^{(\mathbb{N})}, +, \times)$. Pour ce faire, on doit d'abord montrer que le corps $\mathbb{K}$ *s'identifie naturellement* à un sous-anneau de $\mathbb{K}^{(\mathbb{N})}$.

Définition 1.3 – *On appelle polynôme constant un polynôme de degré zéro ou $-\infty$. En d'autres termes, un polynôme $(a_i)_{i\in\mathbb{N}}$ est constant si, pour $i \geq 1$, $a_i = 0$.*

Lemme 1.4 – *À tout $a \in \mathbb{K}$ on associe le polynôme constant, noté $(a, 0, \ldots)$, dont le terme d'indice 0 vaut a. L'application*

$$\begin{array}{rccc} i_{\mathbb{K}} & : & \mathbb{K} & \longrightarrow & \mathbb{K}^{(\mathbb{N})} \\ & & a & \mapsto & (a, 0, \ldots) \end{array}$$

est un morphisme injectif d'anneaux dont l'image est l'ensemble des polynômes constants de $\mathbb{K}^{(\mathbb{N})}$. En particulier, l'ensemble des polynômes constants de $\mathbb{K}^{(\mathbb{N})}$ est une sous-anneau de $\mathbb{K}^{(\mathbb{N})}$, isomorphe à $\mathbb{K}$.

Démonstration : Il est facile de vérifier que $i_{\mathbb{K}}$ est un morphisme de groupes. Il est clair que l'image par $i_{\mathbb{K}}$ de l'élément unité de $\mathbb{K}$ est l'élément unité de $\mathbb{K}^{(\mathbb{N})}$. Soient a et b dans $\mathbb{K}$ et $P = (a, 0, \ldots)$ et $Q = (b, 0, \ldots)$ leurs images par $i_{\mathbb{K}}$. Par définition, si $PQ = (c_i)_{i\in\mathbb{N}}$, on a $c_i = \sum_{p+q=i} a_p b_q$, pour $i \in \mathbb{N}$. Ainsi, $c_i = 0$ si $i > 1$ et $c_0 = ab$. On a donc $i_{\mathbb{K}}(ab) = PQ = i_{\mathbb{K}}(a)i_{\mathbb{K}}(b)$. La démonstration est complète. ∎

Remarque 1.5 – Le lemme 1.4 permet une première simplification dans les notations. Un polynôme constant $P = (a, 0, \ldots)$ de $\mathbb{K}^{(\mathbb{N})}$ ($a \in \mathbb{K}$) sera noté, pour simplifier, a : on dit que l'on *identifie* P à a. Naturellement, à proprement parler, a n'est pas un élément de $\mathbb{K}^{(\mathbb{N})}$. Cependant, l'abus de notation que l'on commet ainsi ne prête pas à confusion. En effet, $i_{\mathbb{K}}$ étant une bijection de $\mathbb{K}$ sur l'ensemble des polynômes constants de $\mathbb{K}^{(\mathbb{N})}$, un polynôme constant de $\mathbb{K}^{(\mathbb{N})}$ s'identifie à un élément de $\mathbb{K}$ et un seul. De plus, $i_{\mathbb{K}}$ étant un morphisme d'anneaux, multiplier entre eux deux polynômes constants $P = (a, 0, \ldots)$ et $Q = (b, 0, \ldots)$ ou les éléments de $\mathbb{K}$ auxquels on les identifie revient au-même au sens où, l'élément auquel PQ est identifié est bien le produit ab des éléments a et b auxquels P et Q sont respectivement identifiés. Des remarques semblables s'appliquent à l'addition.

L'introduction d'un élément particulièrement important de $\mathbb{K}^{(\mathbb{N})}$ va nous permettre de simplifier d'avantage les notations. Dans $\mathbb{K}^{(\mathbb{N})}$, on pose $X = (0, 1, 0, \ldots)$, polynôme dont le seul terme non nul est celui d'indice 1 qui vaut 1. L'élément X s'appelle *l'indéterminée* X. Les produits de X avec lui-même et avec les polynômes constants font l'objet du lemme suivant.

Lemme 1.6 – *Soient $i \in \mathbb{N}$ et $a \in \mathbb{K}$; on a :*
1. $X^i = (0, \ldots, 0, 1, 0, \ldots)$ (polynôme dont le seul terme non nul est celui d'indice i qui vaut 1) ;
2. $aX^i = (0, \ldots, 0, a, 0, \ldots)$ (polynôme dont le seul terme éventuellement non nul est celui d'indice i qui vaut a).

Démonstration : 1. On procède par récurrence sur i. Par convention, X^0 est l'identité de $\mathbb{K}^{(\mathbb{N})}$ qui est bien $(1, 0, \ldots)$. Par définition de X, $X = (0, 1, 0, \ldots)$ (polynôme dont le seul terme non nul est celui d'indice 1 qui vaut 1). Supposons le résultat acquis à l'ordre i ; c'est-à-dire que $X^i = (0, \ldots, 0, 1, 0, \ldots)$ (polynôme dont le seul terme non nul est celui d'indice i qui vaut 1). Alors, $X^{i+1} = XX^i$. Posons $XX^i = (c_j)_{j\in\mathbb{N}}$. Par définition du produit dans $\mathbb{K}^{(\mathbb{N})}$, pour $j \in \mathbb{N}$, on a $c_j = \sum_{p+q=j} a_p b_q$, où l'on a posé $X = (a_j)_{j\in\mathbb{N}}$ et $X^i = (b_j)_{j\in\mathbb{N}}$. Comme le seul a_j non nul est $a_1 = 1$, et le seul b_j non nul est $b_i = 1$, pour $j \in \mathbb{N}$, on a $c_j = \sum_{p+q=j} a_p b_q = 0$ si $j \neq i + 1$ et $c_{i+1} = 1$. Donc, on a bien $X^{i+1} = (0, \ldots, 0, 1, 0, \ldots)$ (polynôme dont le seul terme non nul est celui d'indice $i + 1$ qui vaut 1).
2. Rappelons que compte tenu de l'identification adoptée dans la remarque 1.5, la notation

aX^i signifie en fait $(a, 0, \ldots)X^i$. À l'aide du premier point, on montre facilement que $aX^i = (0, \ldots, 0, a, 0, \ldots)$ (polynôme dont le seul terme éventuellement non nul est celui d'indice i qui vaut a). Les détails sont laissés au lecteur en guise d'exercice. ∎

Remarque 1.7 – 1. Soit P un polynôme de $\mathbb{K}^{(\mathbb{N})}$; il existe une famille $a_0, \ldots, a_d$ d'éléments de $\mathbb{K}$ telle que $P = \sum_{i=0}^{d} a_i X^i$. En effet, $P = (a_0, \ldots, a_d, 0, \ldots)$ où d est un entier tel que pour, $i > d$, $a_i = 0$. Dans la pratique, si $P \neq 0$, on choisira pour d le plus petit entier tel que pour, $i > d$, $a_i = 0$, c'est-à-dire qu'on prendra $d = \deg P$. Ainsi, on pourra écrire

$$P = \sum_{i=0}^{d} a_i X^i = a_0 + a_1 X + \ldots + a_d X^d = \sum_{i=0}^{d} a_i X^i = a_0 1 + a_1 X + \ldots + a_d X^d, \text{ avec } a_d \neq 0.$$

Dans ce cas, a_d sera appelé coefficient dominant de P. (Un polynôme non nul dont le coefficient dominant est 1 sera appelé unitaire.) Néanmoins, ce choix de d minimal oblige à distinguer les deux cas $P \neq 0$ et $P = 0$ ce qui est parfois un peu fastidieux. Ainsi, sauf lorsque cela sera mentionné explicitement, une écriture de la forme $P = \sum_{i=0}^{d} a_i X^i = a_0 + a_1 X + \ldots + a_d X^d$ ne supposera pas *a priori* $a_d \neq 0$.
2. L'écriture d'un polynôme sous la forme $\sum_{i=0}^{d} a_i X^i$ est unique au sens suivant : soient P et Q deux polynômes, $P = \sum_{i=0}^{d} a_i X^i$ et $Q = \sum_{i=0}^{e} b_i X^i$ avec $e \geq d$. Alors, si $P = Q$, pour $d < j \leq e$, $b_j = 0$ et $a_j = b_j$ pour $0 \leq j \leq d$. C'est un conséquence immédiate du fait que $(a_0, \ldots, a_d, 0, \ldots) = P = Q = (b_0, \ldots, b_e, 0, \ldots)$.
3. C'est cette nouvelle écriture à l'aide de X que l'on utilisera dans la pratique. Ainsi, on peut réécrire les lois d'addition et de multiplication entre polynômes à l'aide de ces nouvelles notations. Cet exercice simple est laissé au lecteur. Si $P = \sum_{i=0}^{d} a_i X^i$ est un polynôme, pour $0 \leq i \leq d$, le polynôme $a_i X^i$ est appelé monôme de degré i de P et a_i coefficient d'indice i de P. Notons que, si $a \in \mathbb{K}$ (identifié au polynôme constant), on a $aP = \sum_{i=0}^{d} aa_i X^i = aa_0 + aa_1 X + \ldots + aa_d X^d$.

Définition 1.8 – *L'ensemble $\mathbb{K}^{(\mathbb{N})}$ est aussi noté $\mathbb{K}[X]$. L'anneau $(\mathbb{K}[X], +, \times)$ est appelée l'anneau des polynômes en une indéterminée X, à coefficients dans $\mathbb{K}$.*

On a défini plus haut le degré d'un polynôme comme étant un élément de $\mathbb{N} \cup \{-\infty\}$. Comme on va être amené à comparer et à additionner des degrés, il convient de prolonger l'addition et la relation d'ordre de $\mathbb{N}$ à $\mathbb{N} \cup \{-\infty\}$. Pour ce faire, on pose $-\infty < n$, $\forall n \in \mathbb{N}$, $-\infty + n = -\infty$, $\forall n \in \mathbb{N}$ et $-\infty + (-\infty) = -\infty$.

Proposition 1.9 – *Soient $P, Q \in \mathbb{K}[X]$;*
1. $\deg(P + Q) \leq \sup\{\deg P, \deg Q\}$ *;*
2. $\deg(PQ) \leq \deg P + \deg Q$.

Démonstration : Si P ou Q est nul, le résultat est évident compte tenu des conventions prises pour l'addition et la relation d'ordre dans $\mathbb{N} \cup \{-\infty\}$. Supposons donc que P et Q sont non nuls et posons $P = a_0 + a_1 X + \ldots + a_d X^d$, avec $a_d \neq 0$ et $Q = b_0 + b_1 X + \ldots + b_e X^e$, avec $b_e \neq 0$. Comme l'addition et la multiplication sont commutatives, on peut sans perte de généralité permuter les rôles de P et Q. Ainsi, on peut supposer que $d \leq e$. On a alors $P + Q = s_0 + s_1 X + \ldots + s_e X^e$, avec $s_e = a_e + b_e$ si $e = d$ et $s_e = b_e$ si $e > d$. Ceci établit le premier point. D'autre part, $PQ = m_0 + m_1 X + \ldots + m_{d+e} X^{d+e}$, avec $m_{d+e} = a_d b_e$. Ceci démontre le second point. ∎

On termine cette section par *un théorème de transfert*. On appelera ainsi tout théorème qui établit que si le corps $\mathbb{K}$ jouit d'une certaine propriété alors l'anneau $\mathbb{K}[X]$ en jouit aussi.

Théorème 1.10 – *Si $P, Q \in \mathbb{K}[X]$, $\deg(PQ) = \deg P + \deg Q$. En particulier, $\mathbb{K}[X]$ est un anneau intègre.*

Démonstration : Si P ou Q est nul, le résultat est évident. Supposons que P et Q sont non nuls et posons $P = a_0 + a_1X + \ldots + a_dX^d$, avec $a_d \neq 0$ et $Q = b_0 + b_1X + \ldots + b_eX^e$, avec $b_e \neq 0$. On a $PQ = m_0 + m_1X + \ldots + m_{d+e}X^{d+e}$, avec $m_{d+e} = a_db_e$. Comme $\mathbb{K}$ est intègre, on doit avoir $a_db_e \neq 0$. Ceci démontre le premier point. Soient alors deux polynômes P et Q de $\mathbb{K}[X]$ tels que $PQ = 0$. Ce qui précède montre que $-\infty = \deg(PQ) = \deg P + \deg Q$ et donc on doit avoir $-\infty = \deg P$ ou $-\infty = \deg Q$. Donc si $PQ = 0$, soit P soit Q est nul ce qui montre que $\mathbb{K}[X]$ est intègre. ∎

Corollaire 1.11 – *On a $U(\mathbb{K}[X]) \cong U(\mathbb{K})$. Plus precisément, un polynôme P de $\mathbb{K}[X]$ est inversible si et seulement si il existe $a \in \mathbb{K}^*$ tel que $P = a$.*

Démonstration : C'est une conséquence facile du théorème 1.10. ∎

Remarque 1.12 – Il n'est pas difficile de voir que la construction développée dans la présente section s'étend au cas où l'on remplace le corps $\mathbb{K}$ par un anneau commutatif. En fait, tous les énoncés de cette section s'étendent mot-pour-mot si l'on remplace le corps $\mathbb{K}$ par un anneau commutatif $\mathbb{A}$ quelconque, sauf le Théorème 1.10 et le Corollaire 1.11 qui ne s'étendent que si l'on remplace le corps $\mathbb{K}$ par un anneau *intègre*.

2 Arithmétique des anneaux de polynômes sur un corps.

Dans cette section, on se concentre sur les propriétés arithmétiques des anneaux de polynômes sur le corps $\mathbb{K}$.

L'essentiel des propriétés de l'anneau $\mathbb{Z}$ est une conséquence de l'existence d'une division euclidienne. On ne sera donc guère surpris que les propriétés arithmétiques de $\mathbb{Z}$ s'étendent à $\mathbb{K}[X]$ puisque, dans cet anneau aussi, on dispose d'une division euclidienne. C'est d'ailleurs par l'existence d'une telle division que nous commençons notre étude.

2.1 Division euclidienne.

Théorème 2.1.1 – *Soient P, S deux polynômes de $\mathbb{K}[X]$. On suppose que* $\deg S \geq 0$ *(*i.e. *$S \neq 0$). Il existe un unique couple (Q, R) de polynômes de $\mathbb{K}[X]$ tels que*

$$P = QS + R \text{ et } \deg R < \deg S.$$

Démonstration : Unicité. L'unicité est facile : supposons en effet qu'il existe deux couples (Q, R) et (Q', R') de polynômes de $\mathbb{K}[X]$ tels que $P = QS + R = Q'S + R'$, $\deg R < \deg S$ et $\deg R' < \deg S$. Alors, on a $S(Q - Q') = R' - R$. D'après le théorème 1.10 et la proposition 1.9, on a

$$\deg S + \deg(Q - Q') = \deg(R - R') < \deg S.$$

Si l'on suppose $R - R' \neq 0$, alors $Q - Q' \neq 0$ de sorte que $\deg(Q - Q') \geq 0$ et l'inéquation ci-dessus conduit à $\deg S \leq \deg S + \deg(Q - Q') = \deg(R - R') < \deg S$, ce qui est absurde. Donc on doit avoir $R = R'$ et l'intégrité de $\mathbb{K}[X]$ (théo. 1.10) jointe à la non nullité de S assure que $Q = Q'$. On a donc montré que si un tel couple existe, il est unique.
Existence. Si $P = 0$, il suffit de prendre $(Q, R) = (0, 0)$. La démonstration de l'existence d'un tel couple lorsque $\deg P \geq 0$ se fait par récurrence sur l'entier $\deg P$. Si $\deg P = 0$ (*i.e.* P

est un polynôme constant), ou bien $\deg S > 0$ et le couple $(Q, R) = (0, P)$ convient, ou bien $\deg S = 0$ (S est alors un polynôme constant non nul) et le couple $(Q, R) = (P/S, 0)$ convient (noter que P/S est un élément de $\mathbb{K}$). Soit $n \in \mathbb{N}$; supposons le résultat vrai lorsque $\deg P \leq n$, et soit $P = a_0 + a_1X + \ldots + a_{n+1}X^{n+1}$ un polynôme de degré $n+1$ (donc $a_{n+1} \neq 0$). Posons $S = b_0 + \ldots + b_pX^p$ ($b_p \neq 0$). Si $p > n+1$, le couple $(Q, R) = (0, P)$ convient. Sinon, $p \leq n+1$ et le polynôme $(a_{n+1}/b_p)X^{n+1-p}S$ est de degré $n+1$ et de même coefficient dominant que P. Ainsi, $P - (a_{n+1}/b_p)X^{n+1-p}S$ est un polynôme de degré au plus égal à n. On peut donc lui appliquer l'hypothèse de récurrence et obtenir un couple (Q', R') d'éléments de $\mathbb{K}[X]$ tels que

$$P - (a_{n+1}/b_p)X^{n+1-p}S = Q'S + R' \quad \text{et} \quad \deg R' < \deg S.$$

Donc, on a :

$$P = (Q' + (a_{n+1}/b_p)X^{n+1-p})S + R' \quad \text{et} \quad \deg R' < \deg S.$$

Le couple $(Q' + (a_{n+1}/b_p)X^{n+1-p}, R')$ satisfait aux hypothèses requises pour (Q, R). Ceci achève la preuve. ∎

Remarque 2.1.2 – Dans la pratique, la division euclidienne d'un polynôme P par un polynôme non nul S se fait en s'inspirant de la méthode de preuve du théorème 2.1.1. L'exemple suivant illustre cette méthode. Prenons $P = X^5 + 2X^3 - 3X - 2$ et $S = X^3 + X + 1$. Comme dans la démonstration de 2.1.1, on se ramène à la division d'un polynôme de degré strictement plus petit que celui de P en considérant $P - X^2S$ (c'est le $P - (a_{n+1}/b_p)X^{n+1-p}S$ de la démonstration) : on pose $P_1 = P - X^2S = X^3 - X^2 - 3X - 2$. La division de P_1 par S se fait à nouveau par le même procédé de réduction : on considère $P_2 = P_1 - S = -X^2 - 4X - 3$. On est ramené à effectuer la division euclidienne de P_2 par S ; mais celle-ci est immédiate, en effet, on a abouti à la situation où $\deg P_2 < \deg S$ et donc (comme indiqué dans la preuve de 2.1.1), on a $P_2 = 0(X^3 + X + 1) + (-X^2 - 4X - 3)$. En remontant le procédé précédant, on obtient

$$P_1 = S + P_2, \qquad P = X^2S + P_1 = X^2S + S + P_2.$$

Bien sûr, ce qui garantit l'aboutissement de ce procédé algorithmique, c'est qu'il conduit à construire une suite $P = P_0, P_1, P_2, \ldots$ de polynômes tels que $\deg P_0 > \deg P_1 > \deg P_2 \ldots$ de sorte qu'après un nombre fini d'étapes, disons n, on aboutit (pour la première fois) à un polynôme P_n tel que $\deg P_n < \deg S$ (éventuellement $P_n = 0$). Ces polynômes sont liés par des relations du type $P_{i+1} = P_i - M_iS$, où M_i est un monôme convenablement choisi pour que P_i et M_iS aient même degré et même coefficient dominant, de sorte que $\deg P_{i+1} < \deg P_i$. On a :

$$\begin{aligned} P &= P_1 + M_0S \\ &= P_2 + M_1S + M_0S \\ &= \ldots \\ &= P_{n-1} + M_{n-2}S + \ldots + M_1S + M_0S \\ &= P_n + M_{n-1}S + M_{n-2}S + \ldots + M_1S + M_0S \\ &= P_n + (M_{n-1} + M_{n-2} + \ldots + M_1 + M_0)S, \end{aligned}$$

c'est-à-dire que

$$P = QS + R, \quad \text{où} \quad R = P_n \quad \text{et} \quad Q = (M_{n-1} + \ldots + M_1 + M_0).$$

Ce qui précède permet de donner une description très intéressante de l'ensemble des idéaux de $\mathbb{K}[X]$. On commence par une définition.

Définition 2.1.3 – *1. Soient P et S deux polynômes de $\mathbb{K}[X]$. On dit que S divise P, et on note $S|P$, si il existe un polynôme Q de $\mathbb{K}[X]$ tel que $P = QS$.*
2. Soient P et S deux polynômes de $\mathbb{K}[X]$. On dit que P et S sont associés si $P|S$ et $S|P$.

Remarque 2.1.4 – Soient P et S deux polynômes de $\mathbb{K}[X]$.
1. On suppose $S \neq 0$; compte tenu de l'unicité du couple (Q, R) de la division euclidienne de P par S. Dire que $S|P$ équivaut à dire que le reste de la division euclidienne de P par S est nul.
2. Dire que P et S sont associés signifie qu'il existe Q et Q' dans $\mathbb{K}[X]$ tels que $S = QP$ et $P = Q'S$. Donc, $S = 0$ si et seulement si $P = 0$. Si $S \neq 0$, on a $S = QQ'S$ et l'intégrité de $\mathbb{K}[X]$ assure que $QQ' = 1$. Ainsi, Q est une unité de $\mathbb{K}[X]$ et par suite $Q \in \mathbb{K}^*$ (voir 1.11). Réciproquement, si il existe $\lambda \in \mathbb{K}^*$ tel que $S = \lambda Q$, alors il est clair que P et S sont associés. Finalement, deux polynômes P et S sont associés si et seulement si il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda S$.

Théorème 2.1.5 – *L'anneau de polynômes $\mathbb{K}[X]$ est principal.*

Démonstration : D'après le théorème 1.10, $\mathbb{K}[X]$ est intègre. Soit I un idéal de $\mathbb{K}[X]$. Si $I = \{0\}$, alors I est principal, engendré par 0. Supposons $I \neq \{0\}$. Alors, l'ensemble des polynômes non nuls de I est non vide. Par suite l'ensemble $\mathcal{D} = \{\deg P,\ P \in I \setminus \{0\}\}$ est une partie non vide de $\mathbb{N}$ qui admet donc un plus petit élément d. On peut donc considérer dans $I \setminus \{0\}$ un polynôme S de degré d. Si P est un élément quelconque de I, la division euclidienne de P par S conduit à un couple (Q, R) d'éléments de $\mathbb{K}[X]$ tels que $\deg R < \deg S$ et tels que $P = QS + R$. Cette dernière égalité montre que $R \in I$ puisque $P \in I$ et $S \in I$. Mais, $\deg R < \deg S$ oblige à avoir $R = 0$. Ainsi, on a $P = QS$. Ceci montre que $I \subseteq (S)$. Comme la réciproque est évidente, on a $I = (S)$. On a donc montré que $I = (S)$. ∎

Remarque 2.1.6 – Le théorème 2.1.5 montre que $\mathbb{K}[X]$ est principal.
1. Soient alors I et J deux idéaux de $\mathbb{K}[X]$. Il existe deux polynômes P et S tels que $I = (P)$ et $J = (S)$. Il est alors facile de montrer que $I \subseteq J$ si et seulement si $S|P$.
2. Supposons que P et S soient deux polynômes. Alors, ce qui précède montre que $(P) = (S)$ si et seulement si P et S sont associés.
3. Les deux points précédents sont des analogues pour $\mathbb{K}[X]$ des propriétés bien connues de $\mathbb{Z}$ qui assurent que $p\mathbb{Z} \subseteq s\mathbb{Z}$ si et seulement si $s|p$ et que deux entiers s et p sont tels que $p\mathbb{Z} = s\mathbb{Z}$ si et seulement si $s = p$ ou $s = -p$. Notons que l'assertion ($s = p$ ou $s = -p$) est équivalente à l'assertion ($s|p$ et $p|s$). Comme l'ensemble des unités de $\mathbb{Z}$ est $\{-1, 1\}$, ces deux assertions sont encore équivalentes à l'assertion (il existe $\lambda \in U(\mathbb{Z})$ tel que $p = \lambda s$). La situation dans $\mathbb{Z}$ est donc complétement analogue à celle que l'on vient de décrire dans $\mathbb{K}[X]$.

2.2 Plus grand commun diviseur.

Définition 2.2.1 – *Soient $P_1, \ldots, P_n$ des polynômes de $\mathbb{K}[X]$. On dit qu'un polynôme D de $\mathbb{K}[X]$ est un plus grand commun diviseur (p.g.c.d.) de $P_1, \ldots, P_n$ si $(D) = (P_1, \ldots, P_n)$.*

Remarque 2.2.2 – Soient $P_1, \ldots, P_n$ des polynômes de $\mathbb{K}[X]$.
1. Le théorème 2.1.5 assure qu'il existe un p.g.c.d. de $P_1, \ldots, P_n$.
2. La remarque 2.1.6 permet de lier deux p.g.c.d. de $P_1, \ldots, P_n$. En effet, supposons que D soit un tel p.g.c.d. et soit P un autre élément de $\mathbb{K}[X]$. Cette remarque assure que P est p.g.c.d. de $P_1, \ldots, P_n$ si et seulement si D et P sont associés.

Le théorème suivant donne une caractérisation plus intuitive (et plus conforme au vocabulaire) de la notion de p.g.c.d.

Théorème 2.2.3 – *Soient $n \in \mathbb{N}^*$ et $P_1, \ldots, P_n$ des éléments de $\mathbb{K}[X]$. Un polynôme D est un p.g.c.d. des polynômes $P_1, \ldots, P_n$ si et seulement si D satisfait les deux propriétés suivantes :*
1. D divise les polynômes $P_1, \ldots, P_n$;
2. si P divise les polynômes $P_1, \ldots, P_n$, alors P divise D.

Démonstration : Soit $D \in \mathbb{K}[X]$.
1. On suppose que D est un p.g.c.d. de $P_1, \ldots, P_n$: $(D) = (P_1, \ldots, P_n)$. Soit $1 \leq i \leq n$; l'inclusion $(D) \supseteq (P_1, \ldots, P_n) \supseteq (P_i)$ assure que D divise P_i. L'inclusion $(D) \subseteq (P_1, \ldots, P_n)$ assure qu'il existe $Q_1, \ldots, Q_n \in K[X]$ tels que $D = P_1Q_1 + \ldots + P_nQ_n$. Ainsi, si P est un diviseur commun aux polynômes $P_1, \ldots, P_n$, il doit aussi diviser D. Ceci montre que D satisfait aux deux propriétés de l'énoncé.
2. On démontre, à présent, que si D vérifie les deux propriétés de l'énoncé, alors $(D) = (P_1, \ldots, P_n)$. Supposons donc que D vérifie les deux propriétés de l'énoncé. Pour $1 \leq i \leq n$, D divise P_i, donc $(P_i) \subseteq (D)$. Il s'ensuit que $(P_1, \ldots, P_n) \subseteq (D)$. D'autre part, soit $P \in \mathbb{K}[X]$ tel que $(P) = (P_1, \ldots, P_n)$ (cf. Théorème 2.1.5). Alors, pour $1 \leq i \leq n$, P divise P_i. Donc, par hypothèse, P divise D, c'est-à-dire que $(D) \subseteq (P) = (P_1, \ldots, P_n)$. ∎

On passe maintenant à la notion de polynômes premiers entre eux.

Définition 2.2.4 – *Soit $n \in \mathbb{N}$, $n \geq 2$. Soient $P_1, \ldots, P_n$ des polynômes de $\mathbb{K}[X]$. On dit que les polynômes $P_1, \ldots, P_n$ sont premiers entre eux si 1 est un p.g.c.d. de $P_1, \ldots, P_n$.*

Théorème 2.2.5 – *Soit $n \in \mathbb{N}$, $n \geq 2$. Les polynômes $P_1, \ldots, P_n$ de $\mathbb{K}[X]$ sont premiers entre eux si et seulement si il existe des polynômes $Q_1, \ldots, Q_n$ de $\mathbb{K}[X]$ tels que $P_1Q_1 + \ldots + P_nQ_n = 1$.*

Démonstration : D'après 2.2.1, les polynômes $P_1, \ldots, P_n$ sont premiers entre eux si et seulement si $(P_1, \ldots, P_n) = (1)$. Ainsi, il reste à montrer que $(1) = (P_1, \ldots, P_n)$ si et seulement si il existe $Q_1, \ldots, Q_n$ de $K[X]$ tels que $P_1Q_1 + \ldots + P_nQ_n = 1$. Cette dernière équivalence est un exercice facile. ∎

Corollaire 2.2.6 – **Lemme de Gauss.**
Soient $P, Q, Q' \in \mathbb{K}[X]$; si P divise QQ' et si P et Q sont premiers entre eux, alors P divise Q'.

Démonstration : Puisque $P|QQ'$, il existe $S \in \mathbb{K}[X]$ tel que $PS = QQ'$. Puisque P et Q sont premiers entre eux, il existe $U, V \in \mathbb{K}[X]$ tels que $PU + QV = 1$. Ainsi, $PUQ' + QVQ' = Q'$ et comme $PS = QQ'$, il vient $P(UQ' + SV) = Q'$. ∎

Corollaire 2.2.7 – *Soient $P, Q, S \in \mathbb{K}[X]$; si P et Q sont premiers entre eux et divisent S, alors PQ divise S.*

Démonstration : Par hypothèse, il existe des polynômes P', Q', U, V tels que $PU + QV = 1$, $S = PP' = QQ'$. Il vient alors $S = PUS + QVS = PUQQ' + QVPP' = PQ(UQ' + VP')$. ∎

Corollaire 2.2.8 – *Soient $P, Q, Q' \in \mathbb{K}[X]$; si P et Q sont premiers entre eux et si P et Q' sont premiers entre eux, alors P et QQ' sont premiers entre eux.*

Démonstration : Les hypothèses assurent qu'il existe des polynômes U, V, U', V' tels que $PU + QV = 1$ et $PU' + Q'V' = 1$. Il vient alors (en multipliant ces deux identités) $(PU + QV)(PU' + Q'V') = PUPU' + PUQ'V' + QVPU' + QVQ'V' = P(UPU' + UQ'V' + QVU') + QQ'VV' = 1$, ce qui montre que P et QQ' sont premiers entre eux. ∎

Dans ce qui suit, on décrit un procédé algorithmique de calcul d'un p.g.c.d. de deux polynômes. Cet algorithme s'appelle *algorithme d'Euclide* ; comme son nom l'indique, il repose sur l'existence d'une division euclidienne dans $\mathbb{K}[X]$.

Remarque 2.2.9 – Soient P et S deux polynômes de $\mathbb{K}[X]$. Si $S = 0$, alors il est clair que P et S admettent P (et tous ses associés) pour p.g.c.d..

On commence par énoncer un lemme sur lequel repose l'algorithme d'Euclide.

Lemme 2.2.10 – *Soient P et S deux polynômes de $\mathbb{K}[X]$. Si Q et R sont deux polynômes tels que $P = QS + R$, alors un polynôme D est p.g.c.d. de P et S si et seulement si il est p.g.c.d. de S et R.*

Démonstration : L'égalité $P = QS + R$ montre que $(P, S) = (S, R)$. Le résultat est donc une conséquence immédiate de 2.2.1. ∎

Algorithme d'Euclide. Soient $P, S \in \mathbb{K}[X]$, tels que $S \neq 0$. Posons $S = R_0$ (pour des raisons qui apparaîtront claires plus tard). On peut effectuer la division euclidienne de P par S ; il existe des polynômes Q_1 et R_1 tels que

$$P = Q_1 R_0 + R_1, \quad \text{et} \quad \deg R_1 < \deg R_0.$$

D'après 2.2.10, D est p.g.c.d. de P et $S = R_0$ si et seulement si il est p.g.c.d. de R_0 et R_1. Si $R_1 = 0$, on obtient que $S = R_0$ est p.g.c.d. de P et S. Sinon, on peut effectuer la division euclidienne de R_0 par R_1 ; il existe des polynômes Q_2 et R_2 tels que

$$R_0 = Q_2 R_1 + R_2, \quad \text{et} \quad \deg R_2 < \deg R_1.$$

D'après 2.2.10, D est p.g.c.d. de P et $S = R_0$ si et seulement si il est p.g.c.d. de R_1 et R_2. Si $R_2 = 0$, on obtient que R_1 est p.g.c.d. de P et S. Sinon, on peut effectuer la division euclidienne de R_1 par R_2, etc.. Bien sûr, cet algorithme doit aboutir nécessairement à un reste nul puisque les degrés des restes successifs forment une suite d'entiers strictement décroissante. On construit donc ainsi deux suites finies $Q_1, \ldots, Q_{n+1}$ et $R_0, \ldots, R_{n+1}$ telles que $R_i = 0$ si et seulement si $i = n + 1$ et

$$P = Q_1 R_0 + R_1,\ R_0 = Q_2 R_1 + R_2,\ R_1 = Q_3 R_2 + R_3,\ \ldots, R_{n-2} = Q_n R_{n-1} + R_n,\ R_{n-1} = Q_{n+1} R_n.$$

Ce qui précède montre alors que le dernier reste non nul R_n de ces divisions successives est un p.g.c.d. de P et S.

2.3 Factorialité de l'anneau de polynômes sur un corps.

Dans cette sous-section, on continue l'étude arithmétique de $\mathbb{K}[X]$. On montre ici que, comme dans l'anneau $\mathbb{Z}$, un polynôme peut être factorisé en produit de polynômes dits *irréductibles*, et ceci de manière (essentiellement) *unique*.

Définition 2.3.1 – *Un polynôme P de $\mathbb{K}[X]$ est dit irréductible si il vérifie les deux conditions suivantes.*
1. Le polynôme P est non constant.
2. Si il existe $S, Q \in K[X]$ tels que $P = QS$, alors Q ou S est un polynôme constant.

Remarque 2.3.2 – Il est facile de montrer qu'un polynôme P de $\mathbb{K}[X]$ est irréductible si et seulement si
1. il est non constant ;
2. ses seuls diviseurs sont ces associés (c-à-d les λP pour $\lambda \in \mathbb{K}^*$).

Remarque 2.3.3 – Les assertions suivantes sont faciles à démontrer.
1. Si $P \in \mathbb{K}[X]$ est irréductible, alors pour tout $\lambda \in \mathbb{K}^*$, λP est irréductible.
2. Soit P dans $\mathbb{K}[X]$ irréductible et $S \in \mathbb{K}[X]$. Si P ne divise pas S, alors P et S sont premiers entre eux (ces deux cas s'excluant mutuellement).
3. Deux polynômes irréductibles sont, soit associés, soit premiers entre eux (ces deux cas s'excluant mutuellement).

Exemple 2.3.4 –
1. Tout polynôme de degré un est irréductible.
2. Le polynôme $X^2 - 2 \in \mathbb{Q}[X]$ est irréductible ; cependant, le polynôme $X^2 - 2 \in \mathbb{R}[X]$ n'est pas irréductible. De même, le polynôme $X^2 + 1 \in \mathbb{R}[X]$ est irréductible ; mais, le polynôme $X^2 + 1 \in \mathbb{C}[X]$ n'est pas irréductible.

Lemme 2.3.5 – *Soient $P, Q, Q' \in \mathbb{K}[X]$ où P est irréductible. Si P divise QQ', alors il divise Q ou Q'.*

Démonstration : Compte tenu de 2.3.3, si P ne divise pas Q, il doit être premier avec Q, de sorte que le lemme de Gauss 2.2.6 montre que $P|Q'$. ∎

Théorème 2.3.6 – *Soit $P \in \mathbb{K}[X]$ un polynôme de degré supérieur ou égal à 1.*
1. Il existe un entier n dans $\mathbb{N}^*$ et des polynomes $P_1, \ldots, P_n$ irréductibles dans $\mathbb{K}[X]$ tels que $P = P_1 \ldots P_n$.
2. Si m et n sont des entiers de $\mathbb{N}^*$ et $P_1, \ldots, P_n, Q_1, \ldots, Q_m$ des polynômes irréductibles de $\mathbb{K}[X]$ tels que $P = P_1 \ldots P_n = Q_1 \ldots Q_m$. Alors, $m = n$ et il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que, pour tout $i \in \{1, \ldots, n\}$, P_i et $Q_{\sigma(i)}$ soient associés.

Démonstration : 1. La preuve se fait par récurrence sur le degré de P. Si P est de degré 1, il est irréductible comme on l'a dit en 2.3.3. Le résultat est donc acquis. Supposons le résultat vrai pour tout polynôme de degré n, $n \geq 1$. Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n+1$. Si P est irréductible, il n'y a rien à prouver. Sinon, il existe S et Q dans $\mathbb{K}[X]$ tels que $P = QS$ et tels que ni Q ni S ne soit constant. On en déduit que $1 \leq \deg Q, \deg S \leq n$. L'hypothèse de récurrence assure que S et Q peuvent s'écrire comme produit de polynômes irréductibles ; il s'ensuit aussitôt que leur produit $P = QS$ aussi.
2. Exercice (plutôt délicat). ∎

Remarque 2.3.7 – Soit $P \in \mathbb{K}[X]$ un polynôme de degré supérieur ou égal à 1, une décomposition de P de la forme $P = P_1 \ldots P_n$ avec $n \in \mathbb{N}^*$ et $P_1, \ldots, P_n$ polynômes irréductibles dans $\mathbb{K}[X]$ s'appelle une décomposition de P en produit d'irréductibles.
2. Dans $\mathbb{R}[X]$, on a $2X^2 - 4 = (2X + 2\sqrt{2})(X - \sqrt{2}) = (\sqrt{2}X + 2)(\sqrt{2}X - 2)$; le polynôme

$2X^2 - 4$ admet donc deux décompositions distinctes en produit d'irréductibles. Cependant, conformément au second point du théorème 2.3.6, ces deux décompositions sont *presque* les mêmes au sens où $2X + 2\sqrt{2}$ et $\sqrt{2}X + 2$ sont associés ainsi que $X - \sqrt{2}$ et $\sqrt{2}X - 2$.
3. Dans la pratique, si un polynôme P de degré supérieur ou égal à 1 admet une décomposition de la forme $P = P_1, \ldots, P_n$ en produits d'irréductibles, on sera souvent amené à regrouper les polynômes de la liste $P_1, \ldots, P_n$ qui sont associés. On aboutira alors à une expression de P de la forme $P = UQ_1^{\alpha_1} \ldots Q_s^{\alpha_s}$, où U est une unité de $\mathbb{K}[X]$ (c'est-à-dire $U \in \mathbb{K}^*$ d'après le corollaire 1.11) et où les polynômes $Q_1, \ldots, Q_s$ sont irréductibles et deux-à-deux non associés. Par exemple, dans $\mathbb{R}[X]$, si $P = (2X - 4)(X + 1)(6X - 12)$, on écrira plutôt $P = 12(X - 2)^2(X + 1)$.

3 Fonctions polynômiales ; racines d'un polyôme.

Dans la suite, on note $\mathcal{F}(\mathbb{K})$ l'ensemble des fonctions de $\mathbb{K}$ dans $\mathbb{K}$.

3.1 Fonctions polynômiales.

Définition 3.1.1 – *Soit P un polynôme de $\mathbb{K}[X]$ et $a_0, \ldots, a_n \in \mathbb{K}$ tels que $P = a_0 + a_1X + \ldots + a_nX^n$. On appelle fonction polynômiale associée à P la fonction $\widetilde{P} \in \mathcal{F}(\mathbb{K})$ définie par*

$$\begin{array}{rccc} \widetilde{P} & : & \mathbb{K} & \longrightarrow & \mathbb{K} \\ & & x & \mapsto & a_0 + a_1x + \ldots + a_nx^n. \end{array}$$

On dispose ainsi d'une application $\mathbb{K}[X] \longrightarrow \mathcal{F}(\mathbb{K})$ qui à tout polynôme P fait correspondre la fonction $\widetilde{P}$ associée à P. Rappelons que l'ensemble $\mathcal{F}(\mathbb{K})$ des fonctions de $\mathbb{K}$ dans $\mathbb{K}$ est un anneau pour les l.c.i. d'addition et de multiplication usuelles des fonctions. Ainsi, si f et g sont dans $\mathcal{F}(\mathbb{K})$, on note $f+g$ l'application de $\mathcal{F}(\mathbb{K})$ qui à $x \in \mathbb{K}$ associe $f(x)+g(x)$ et fg l'application de $\mathcal{F}(\mathbb{K})$ qui à $x \in \mathbb{K}$ associe $f(x)g(x)$. De plus, la fonction neutre pour l'addition est celle qui à tout x associe 0 (fonction nulle) et la fonction neutre pour la multiplication est celle qui à tout x associe 1 (fonction constante égale à 1). Notons qu'à tout élément a de $\mathbb{K}$ on peut associer dans $\mathcal{F}(\mathbb{K})$ la fonction constante égale à a qui à tout $x \in \mathbb{K}$ associe a ; on dispose donc d'un morphisme injectif d'anneaux de $\mathbb{K}$ dans $\mathcal{F}(\mathbb{K})$ qui à $a \in \mathbb{K}$ associe la fonction constante égale à a.

Proposition 3.1.2 – *L'application $\mathbb{K}[X] \longrightarrow \mathcal{F}(\mathbb{K})$ qui à tout polynôme P fait correspondre la fonction $\widetilde{P}$ associée à P est un morphisme d'anneaux.*

Démonstration : La preuve est un simple calcul laissé en exercice. ∎

Remarque 3.1.3 – L'application $\mathbb{K}[X] \longrightarrow \mathcal{F}(\mathbb{K})$ qui à tout polynôme P fait correspondre la fonction $\widetilde{P}$ associée à P étant un morphisme d'anneaux, son image est une sous-anneau de $\mathcal{F}(\mathbb{K})$. Ce sous-anneau est appelé ensemble des fonctions polynômiales de $\mathbb{K}$ dans $\mathbb{K}$; il sera notée $\mathcal{F}_{\text{pol}}(\mathbb{K})$. On dispose ainsi d'un morphisme surjectif d'anneaux :

$$\begin{array}{rccc} \varphi & : & \mathbb{K}[X] & \longrightarrow & \mathcal{F}_{\text{pol}}(\mathbb{K}) \\ & & P & \mapsto & \widetilde{P} \end{array}.$$

Une de nos préoccupations essentielles dans ce chapitre va être l'étude de l'injectivité de φ. On perd rapidement tout espoir que φ soit injective en général si l'on observe l'exemple suivant.

Exemple 3.1.4 – Soit p un entier premier. Posons $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$. Ainsi, $\mathbb{K}$ est un corps fini de cardinal p ; le groupe des unités de $\mathbb{K}$ est un groupe fini d'ordre $p-1$. Pour tout $x \in U(\mathbb{K}) = \mathbb{K} \setminus \{0\}$, on a $x^{p-1} = 1$ (cf. exercice 5.9 du chapitre III). Par conséquent, pour tout x dans $\mathbb{K}$, on a $x^p - x = 0$. Ainsi, le polynôme $X^p - X \in \mathbb{K}[X]$ qui est non nul a pour image par φ la fonction nulle. En fait, en utilisant le théorème de Lagrange (voir l'exercice 1.3.5 de la section X.1), on peut montrer que le résultat ci-dessus reste vrai pour tout corps fini de cardinal p, $p \in \mathbb{N}^*$. Ainsi, si $\mathbb{K}$ est un corps fini, l'application φ n'est jamais injective.

3.2 Racines d'un polynôme.

Soit $P \in \mathbb{K}[X]$ un polynôme et $\widetilde{P}$ la fonction polynomiale associée à P. Pour tout $a \in \mathbb{K}$, on s'autorise l'abus de langage qui consiste à noter $P(a)$ au lieu de $\widetilde{P}(a)$ l'image de a par la fonction polynomiale $\widetilde{P}$. Cet abus ne prête pas à confusion.

Définition 3.2.1 – *Soit $P \in \mathbb{K}[X]$; on appelle racine de P tout élément $a \in \mathbb{K}$ tel que $P(a) = 0$, c'est-à-dire tout élément de $\mathbb{K}$ qui annule la fonction polynomiale associée à P.*

Lemme 3.2.2 – *Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$; a est racine de P si et seulement si $X - a$ divise P.*

Démonstration : La division euclidienne de P par $X - a$ fournit deux polynômes Q et R tels que $P = (X-a)Q + R$ et $\deg R < 1$. Ainsi, on a nécessairement $R \in \mathbb{K}$. Comme φ est un morphisme d'anneaux, l'égalité $P = (X-a)Q + R$ conduit à $\widetilde{P} = (\widetilde{X-a})\widetilde{Q} + \widetilde{R}$. La fonction $\widetilde{X-a} \in \mathcal{F}(\mathbb{K})$ est définie par $x \in K \mapsto x - a$ et la fonction $\widetilde{R} \in \mathcal{F}(K)$ est la fonction constante égale à $R \in \mathbb{K}$. Ainsi, $\widetilde{P} = (\widetilde{X-a})\widetilde{Q} + \widetilde{R}$ implique que $P(a) = \widetilde{P}(a) = (\widetilde{X-a})(a)\widetilde{Q}(a) + \widetilde{R}(a) = R$. Donc, $R = P(a)$, et le résultat s'en déduit. ∎

Théorème 3.2.3 – *Soit $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$; si $\deg P \leq n$ et si P admet dans $\mathbb{K}$ $n+1$ racines distinctes, alors P est le polynôme nul.*

Démonstration : On procède par récurrence sur $n \in \mathbb{N}$. La propriété est claire si $n = 0$ car P est alors un polynôme constant. Supposons le résultat vrai pour un entier n, et soit P un polynôme de degré majoré par $n+1$ et possédant $n+2$ racines distinctes. Notons $a_1, \ldots, a_{n+2}$ les $n+2$ racines distinctes de P ; d'après 3.2.2, il existe $Q \in K[X]$ tels que $P = (X - a_{n+2})Q$. De cette égalité, on déduit facilement que $\deg Q \leq n$ et que Q admet $a_1, \ldots, a_{n+1}$ pour racines. Par hypothèse de récurrence, ceci montre que $Q = 0$. Donc, on a $P = 0$. ∎

Théorème 3.2.4 – *Soit $\mathbb{K}$ un corps infini ; alors le morphisme $\varphi : \mathbb{K}[X] \longrightarrow \mathcal{F}_{\mathrm{pol}}(\mathbb{K})$, $P \mapsto \widetilde{P}$ est un isomorphisme.*

Démonstration : Par définition φ est un morphisme surjectif d'anneaux ; il reste à démontrer qu'il est injectif. Soit P un polynôme de $\mathbb{K}[X]$ dont la fonction polynômiale associée est identiquement nulle. Si $n \in \mathbb{N}$ est un entier tel que $\deg P \leq n$, alors on peut trouver $n+1$ éléments distincts de $\mathbb{K}$ qui annulent $\widetilde{P}$ puisque $\mathbb{K}$ est infini. Ces $n+1$ éléments distincts de K sont donc $n+1$ racines distinctes de P et le théorème 3.2.3 assure alors que $P = 0$. ∎

Remarque 3.2.5 – Bien sûr, le théorème 3.2.4 montre que, si $\mathbb{K}$ est un corps infini, on peut identifier, par φ, un polynôme et la fonction polynomiale qui lui est associée. Ceci s'applique en particulier lorsque $\mathbb{K}$ est $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. En utilisant 3.1.4, on conclut que φ est injective si et seulement si $\mathbb{K}$ est infini .

On définit, à présent, la dérivée formelle d'un polynôme.

Définition 3.2.6 –
1. Soit $P = a_0 + a_1X + \ldots + a_dX^d$ un polynôme de $\mathbb{K}[X]$, de degré $d \geq 1$. On appelle polynôme dérivé de P le polynôme, noté P', défini par $P' = a_1 + 2a_2X + \ldots + da_dX^{d-1}$. On étend cette définition aux polynômes constants en posant $P' = 0$ pour tout polynôme constant $P \in \mathbb{K}[X]$.
2. On pose $P^{(0)} = P$, $P^{(1)} = P'$ et, pour $k \geq 1$, $P^{(k+1)} = (P^{(k)})'$. Pour $k \in \mathbb{N}$, le polynôme $P^{(k)}$ s'appelle la dérivée k-ème de P.

Il est clair alors que, si $a \in \mathbb{K}$ et si $P, Q \in \mathbb{K}[X]$, on a : $(aP)' = aP'$ et $(P+Q)' = P' + Q'$. On dispose, par ailleurs, de la formule de Leibnitz qui est l'objet du lemme suivant.

Lemme 3.2.7 – *Soient $k \in \mathbb{N}^*$, $P, Q \in \mathbb{K}[X]$; on a $(PQ)^{(k)} = \sum_{i=0}^{k} C_k^i P^{(i)} Q^{(k-i)}$.*

Démonstration : Elle se fait par récurrence sur k ; les détails sont laissés au lecteur. ∎

Remarque 3.2.8 – Lorsque le corps n'est pas de caractéristique nulle, des choses étranges peuvent se produire. Par exemple, le polynôme $P = X^2 - \overline{1} \in \mathbb{F}_2[X]$ admet pour polynôme dérivé le polynôme nul : $P' = \overline{2}X = \overline{0}$. (On rappelle que, par définition, $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. On rappelle, en outre, que la caractéristique d'un anneau a été introduite et étudiée à l'Exercice 5.6 de la partie III.)

On va maintenant établir la formule de Taylor qui sera utile plus loin pour caractériser l'ordre d'une racine. Une restriction sur $\mathbb{K}$ est nécessaire pour que cette formule soit valide. La remarque suivante explicite le problème qui se pose.

Remarque 3.2.9 – Dans cette remarque, on utilise des notions introduites à l'exercice 5.6 de la partie III et, en particulier, la notion de *caractéristique d'un anneau.*

Soit A un anneau. Si $n \in \mathbb{N}^*$ et $a \in A$, on note $n.a$ ou plus simplement na la somme de n copies de a. Par abus de notation, on pose alors $n = n1_A \in A$. Il faut bien prendre garde alors que $n = n1_A = n.1_A \in A$ n'est pas nécessairement non nul.
1-er cas : Si A est de caractéristique 0, alors par définition même de la caractéristique, $n.1_A \neq 0$.
2-nd cas : Si A est de caractéristique p non nulle, alors par définition, $n.1_A = 0_A$ si et seulement si $n \in p\mathbb{Z}$.
Supposons maintenant que $\mathbb{K}$ soit un corps. S'il est de caractéristique nulle, pour tout $n \in \mathbb{N}^*$, l'élément $n = n1_{\mathbb{K}} = n.1_{\mathbb{K}} \in \mathbb{K}$ est non nul, donc inversible et on note $1/n \in \mathbb{K}$ son inverse. Attention, la notation $1/n$ est un abus de langage. Bien sûr, si $\mathbb{K}$ n'est pas de caractéristique nulle, $n \in \mathbb{K}$ n'est pas nécessairement non nul et donc n'a pas nécessairement d'inverse.

Théorème 3.2.10 – **Formule de Taylor.** *Soit $\mathbb{K}$ un corps de caractéristique nulle. Si P est un polynôme de degré $d \geq 0$ de $\mathbb{K}[X]$ et si $a \in K$, on a*

$$P = \sum_{k=0}^{d} \frac{1}{k!} P^{(k)}(a)(X-a)^k.$$

Démonstration : Le résultat est facile à démontrer lorsque P est un monôme (en utilisant la formule du binôme). Le cas général s'en déduit aisément. Les détails sont laissés au lecteur. ∎

Soit P un polynôme de $\mathbb{K}[X]$ et $a \in \mathbb{K}$ une racine de P. Le lemme 3.2.2 assure que $X - a$ divise P. On précise ce résultat en posant la définition suivante.

Définition 3.2.11 – *Soit P un polynôme de $\mathbb{K}[X]$ et $a \in \mathbb{K}$ une racine de P. On dit que a est racine de P (d'ordre) de multiplicité m si et seulement si $(X-a)^m$ divise P et $(X-a)^{m+1}$ ne divise pas P.*

Remarque 3.2.12 – Soit P un polynôme non nul de $\mathbb{K}[X]$.
1. Si $a \in \mathbb{K}$ est une racine de P, le lemme 3.2.2 montre que la multiplicité de a est au moins égale à 1. Soit m la multiplicité de a ; alors, il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^m Q$ et $X-a$ ne divise pas Q. En particulier, on a $Q(a) \neq 0$ d'après 3.2.2.
2. Par convention, si a n'est pas racine de P, on dit que a est racine de multiplicité 0. Il est clair alors que si $a \in \mathbb{K}$, et si a est racine de P d'ordre de multiplicité m, alors $0 \leq m \leq d = \deg P$.

Le résultat suivant permet de caractériser l'ordre de multiplicité d'une racine a de P à l'aide des polynômes dérivés de P. Comme ce résultat utilise la formule de Taylor, il n'est vrai que si $\mathbb{K}$ est de caractéristique nulle.

Théorème 3.2.13 – *On suppose que le corps $\mathbb{K}$ est de caractéristique 0. Soit P un polynôme non nul de $\mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$. Alors, a est racine de P de multiplicité $m \in \mathbb{N}$ si et seulement si $P(a) = P'(a) = \ldots = P^{(m-1)}(a) = 0$ et $P^{(m)}(a) \neq 0$.*

Démonstration : Supposons que $P(a) = P'(a) = \ldots = P^{(m-1)}(a) = 0$ et $P^{(m)}(a) \neq 0$. Comme P est non nul, la formule de Taylor montre que $0 \leq m \leq d := \deg P$. De plus, on a $P = (X-a)^m Q$, où $Q = (1/m!)P^{(m)}(a) + \ldots + (1/d!)P^{(d)}(a)(X-a)^{d-m}$. Il est clair que $Q(a) = (1/m!)P^{(m)}(a) \neq 0$, ce qui assure que Q n'est pas divisible par $X-a$. Ceci montre que a est racine de P d'ordre de multiplicité m.
Réciproquement, supposons que a est racine de P d'ordre de multiplicité m (notons que $0 \leq m \leq d$). Dans la division euclidienne de P par $(X-a)^m$, le reste doit être nul. Or, la formule de Taylor assure que

$$P = \left(\sum_{k=m}^{d} \frac{1}{k!} P^{(k)}(a)(X-a)^{k-m} \right) (X-a)^m + \sum_{k=0}^{m-1} \frac{1}{k!} P^{(k)}(a)(X-a)^k.$$

On doit donc avoir $R = \sum_{k=0}^{m-1} (1/k!)P^{(k)}(a)(X-a)^k = 0$. Ceci entraîne que $P^{(k)}(a) = 0$ pour $0 \leq k \leq m-1$ (voir exercices). Par ailleurs, on a nécessairement $P^{(m)}(a) \neq 0$ car sinon, d'après l'identité ci-dessus, on aurait $P = (\sum_{k=m}^{d} (1/k!)P^{(k)}(a)(X-a)^{k-m})(X-a)^m = (\sum_{k=m+1}^{d} (1/k!)P^{(k)}(a)(X-a)^{k-m})(X-a)^m$, ce qui assurerait que P est divisible par $(X-a)^{m+1}$, contredisant ainsi le fait que a est racine de P d'ordre de multiplicité m. ∎

4 *Exercices.*

§A - Divisibilité, p.g.c.d.

Exercice 4.1 –
1. Effectuer la division euclidienne de $P = X^4 + 6X^3 + 10X^2 + 3X - 6$ par $S = X^2 + 3X$ dans $\mathbb{R}[X]$.
2. Effectuer la division euclidienne de $P = X^3 - 3iX + 5(1+i)$ par $S = X - 1 + i$ dans $\mathbb{C}[X]$.

Exercice 4.2 – Soit $\phi \in \mathbb{R}$. Pour tout $n \in \mathbb{N}^*$, on pose $P_n = X^{n+1}\cos(n-1)\phi - X^n \cos n\phi - X\cos\phi + 1$. Montrer que pour tout $n \in \mathbb{N}^*$, P_n est divisible par $S = X^2 - 2X\cos\phi + 1$ et expliciter le polynôme Q tel que $P = QS$.

Exercice 4.3 – Dans les trois cas suivants, déterminer les p.g.c.d. de P et S dans $\mathbb{R}[X]$;
1. $P = X^5 + X^4 + 2X^3 - 2X + 3$, $S = X^4 + 3X^3 + 7X^2 + 8X + 6$;
2. $P = X^5 - X^4 + 2X^3 + 1$, $S = X^5 + X^4 + 2X^2 - 1$;
3. $P = X^4 + 2X^3 - 11X^2 - 12X + 36$, $S = 4X^3 + 6X^2 - 22X - 12$.

Exercice 4.4 – Soient m et n dans $\mathbb{N}^*$ tels que $m > n$.
1. Effectuer la division euclidienne dans $\mathbb{N}$ de m par n et en déduire la division euclidienne de $P = X^m - 1$ par $S = X^n - 1$ dans $\mathbb{R}[X]$.
2. Déterminer les p.g.c.d. des polynômes $P = X^m - 1$ et $S = X^n - 1$ de $\mathbb{R}[X]$.
3. Déterminer les p.g.c.d. de $X^7 + X^6 + \ldots + X^2 + X + 1$ et $X^5 + X^4 + \ldots + X + 1$.

Exercice 4.5 – On note $\mathbb{K}$ un corps de caractéristique nulle. Déterminer tous les polynômes $P \in \mathbb{K}[X]$ tels que P' divise P.

B - Equations diophantiennes.

Exercice 4.6 – On note $\mathbb{K}$ un corps.
1. Soient P et S deux polynômes non nuls et non tous deux constants de $\mathbb{K}[X]$ et premiers entre eux. Montrer qu'il existe un couple $(U, V) \in \mathbb{K}[X] \times \mathbb{K}[X]$ et un seul tel que $UP + VS = 1$ et $\deg U < \deg S$, $\deg V < \deg P$.
2. Montrer que les polynômes $P = X^7 - X - 1$ et $S = X^5 + 1$ sont premiers entre eux et trouver $(U, V) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tel que $UP + VS = 1$ et $\deg U < \deg S$, $\deg V < \deg P$.

Exercice 4.7 – Soit $\mathbb{K}$ un corps. Déterminer tous les couples $(U, V) \in \mathbb{K}[X]^2$ tel que $X^n U + (1 - X)V = 1$, où $n \geq 1$.

C - Racines.

Exercice 4.8 – Démontrer que $X^{3p+2} + X^{3q+1} + X^{3r} \in \mathbb{R}[X]$ est divisible par $X^2 + X + 1$ pour tout $(p, q, r) \in \mathbb{N}^3$.

Exercice 4.9 –
1. Décomposer le polynôme $P = 2X^3 - (5+6i)X^2 + 9iX + 1 - 3i \in \mathbb{C}[X]$ en produit d'irréductibles sachant qu'il admet une racine réelle.
2. Soient $a, b \in \mathbb{R}$. Déterminer a et b de sorte que le polynôme $P = X^4 + 2X^3 + 3X^2 + aX + b$ admette $1 + i$ pour racine. Pour ces valeurs de a et b, décomposer P dans $\mathbb{R}[X]$.
3. Décomposer dans $\mathbb{R}[X]$ les polynôme suivants :
a) $X^4 + 1$;
b) $X^4 + X^2 + 1$;
c) $(X^2 - X + 1)^2 + 1$.

Exercice 4.10 – Montrer que les polynômes suivants n'ont pas de racines multiples dans $\mathbb{C}$:
a) $X^4 + X$; b) $X^5 - 5X + 1$; c) tout polynôme de la forme $X^2 + bX + c$ où $b^2 \neq 4c$.

Exercice 4.11 – Soit $n \in \mathbb{N}^*$; montrer que le polynôme $P = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$ admet une racine multiple (c'est-à-dire de multiplicité au moins égal à 2).

Exercice 4.12 – Décomposer le polynôme $P = X^5 - 13X^4 + 67X^3 - 171X^2 + 216X - 108 \in \mathbb{R}[X]$ sachant qu'il admet des racines multiples.

Exercice 4.13 – Montrer que $X^3 + X^2 + 1$ est irréductible dans $\mathbb{F}_2[X]$.

Exercice 4.14 – **Le théorème de Wilson par les polynômes.**
Soit p un entier premier et $\mathbb{K} = \mathbb{F}_p$. Montrer que le produit des éléments non nuls de $\mathbb{K}$ est égal à -1. En déduire que $(p-1)! \equiv -1 (\mathrm{mod}\, p)$.
Indication. On pourra considerer les polynômes $P = (X - \overline{1}) \dots (X - \overline{p-1})$ et $Q = X^{p-1} - \overline{1}$ de $\mathbb{F}_p[X]$, montrer qu'ils ont même racines puis en déduire qu'ils sont égaux. On rappelle que si $\mathbb{K}$ est un corps, le nombre de racines d'un polynôme ne peut excéder sont degré.

Exercice 4.15 – Déterminer les racines de $X^2 - \overline{1} \in (\mathbb{Z}/15\mathbb{Z})[X]$.
Indication. On pourra s'aider de la table de multiplication de $\mathbb{Z}/15\mathbb{Z}$.

Exercice 4.16 – Montrer que si $\mathbb{K}$ est un corps commutatif, alors tout sous-groupe fini du groupe des unités de $\mathbb{K}$ est cyclique.

D - Polynômes et fonctions polynomiales pour les corps finis.

Exercice 4.17 – Soit $\mathbb{K}$ un corps fini à q éléments. Calculer le noyau et l'image de l'application $\mathbb{K}[X] \longrightarrow \mathcal{F}(\mathbb{K})$, qui envoie un polynôme sur la fonction polynomiale associée.

Partie VI

Géométrie vectorielle.

Dans toute la suite, $\mathbb{K}$ désigne un corps commutatif.

1 Espaces vectoriels.

Définition 1.1 – *Une structure de $\mathbb{K}$-espace vectoriel sur un ensemble E est la donnée d'une loi de composition interne (l.c.i.) $+ : E \times E \longrightarrow E$, $(x, y) \mapsto x + y$ et d'une loi de composition externe (l.c.e.) à scalaires dans $\mathbb{K}$ $. : \mathbb{K} \times E \mapsto E$, $(\lambda, x) \mapsto \lambda x$ telles que :*
(i) $(E, +)$ soit un groupe abélien (dont le neutre est noté 0) ;
(ii) pour tous $\lambda, \mu \in \mathbb{K}$ et tous $x, y \in E$: $\lambda(x+y) = \lambda x + \lambda y$, $(\lambda+\mu)x = \lambda x + \lambda y$, $\lambda(\mu x) = (\lambda\mu)x$, $1.x = x$.

Exercice 1.2 – *Soit E un $\mathbb{K}$-espace vectoriel. Pour tout $x \in E$ et tout $\lambda \in \mathbb{K}$, on a :*
1. $0.x = 0$ *;*
2. $\lambda.0 = 0$ *;*
3. $(-1).x = -x$.

Exemple 1.3 –
1. Le corps de base $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel : la l.c.i. est l'addition dans $\mathbb{K}$; la l.c.e. est le produit dans $\mathbb{K}$.
2. Pour tout entier $n \in \mathbb{N}^*$, $\mathbb{K}^n$ est un $\mathbb{K}$-espace vectoriel relativement aux lois :

$$\begin{array}{rccc} + & : & \mathbb{K}^n \times \mathbb{K}^n & \longrightarrow & \mathbb{K}^n \\ & & ((x_1, \ldots, x_n), (y_1, \ldots, y_n)) & \mapsto & (x_1 + y_1, \ldots, x_n + y_n) \end{array}$$

et

$$\begin{array}{rccc} . & : & \mathbb{K} \times \mathbb{K}^n & \longrightarrow & \mathbb{K}^n \\ & & (\lambda, (x_1, \ldots, x_n)) & \mapsto & (\lambda x_1, \ldots, \lambda x_n) \end{array} .$$

Soit $x = (x_1, \ldots, x_n) \in \mathbb{K}^n$. Pour $i \in \{1, \ldots, n\}$, on appelle x_i le coefficient d'indice i (ou i-ème coefficient) de x. On note que, pour $n = 1$, on retrouve la structure d'espace vectoriel sur $\mathbb{K}$ définie au premier point.
3. L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est une $\mathbb{K}$-espace vectoriel relativement à la loi de groupe de $\mathbb{K}[X]$ définie au Chapitre V et à la l.c.e. suivante :

$$\begin{array}{rccc} . & : & \mathbb{K} \times \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ & & (\lambda, (a_i)_{i\in\mathbb{N}}) & \mapsto & (\lambda a_i)_{i\in\mathbb{N}} \end{array} .$$

Définition 1.4 –
1. Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f : E \longrightarrow F$ une application. On dit que f est une application linéaire si, pour tout $\lambda \in \mathbb{K}$ et tous $x, y \in E$, $f(x + y) = f(x) + f(y)$ et $f(\lambda x) = \lambda f(x)$.
2. Un endomorphisme est une application linéaire d'un espace vectoriel dans lui-même. Un isomorphisme est une application linéaire bijective. Un automorphisme est un endomorphisme bijectif.

Notation 1.5 – Soient E et F deux $\mathbb{K}$-espaces vectoriels. L'ensemble des applications linéaires de E dans F est noté $\mathcal{L}(E, F)$. L'ensemble des endomorphismes de E est noté $\mathcal{L}(E)$ (ainsi, $\mathcal{L}(E) = \mathcal{L}(E, E)$). L'ensemble des automorphismes de E est noté $GL(E)$.

Définition 1.6 – *Soit E un $\mathbb{K}$-espace vetoriel. Une forme linéaire sur E est une application linéaire de E dans $\mathbb{K}$.*

Exercice 1.7 –
1. Soient E et F deux $\mathbb{K}$-espaces vectoriels. On définit sur $\mathcal{L}(E,F)$ une l.c.i. $\mathcal{L}(E,F) \times \mathcal{L}(E,F) \longrightarrow \mathcal{L}(E,F)$, $(f,g) \mapsto f+g$ et une l.c.e. $\mathbb{K} \times \mathcal{L}(E,F) \longrightarrow \mathcal{L}(E,E)$, $(\lambda, f) \mapsto \lambda f$ à scalaires dans $\mathbb{K}$ par : pour tout $x \in E$, $(f+g)(x) = f(x)+g(x)$ et $(\lambda f)(x) = \lambda f(x)$. Montrer que ces lois munissent $\mathcal{L}(E,F)$ d'une structure de $\mathbb{K}$-espace vectoriel.
2. Montrer que la composition des applications muni $GL(E)$ d'une structure de groupe. Ce groupe est appelé le groupe linéaire de E.

Exercice 1.8 –
1. Soient $n \in \mathbb{N}^*$ et $E_1, \ldots, E_n$ des $\mathbb{K}$-espaces vectoriels. On munit l'ensemble $E = E_1 \times \ldots \times E_n$ d'une l.c.i $+ : E \times E \longrightarrow E$ et d'une l.c.e. $. : \mathbb{K} \times E \longrightarrow$ à scalaires dans $\mathbb{K}$ respectivement définies, pour $\lambda \in \mathbb{K}$ et $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in E$ par $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$ et $\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$. Montrer que les lois ci-dessus munissent E d'une structure de $\mathbb{K}$-espace vectoriel. On appelle E le produit des espaces vectoriels $E_1, \ldots, E_n$.
2. Pour $n \in \mathbb{N}^*$ le $\mathbb{K}$-espace vectoriel $\mathbb{K}^n$ est le produit des espaces vectoriels $\mathbb{K}, \ldots, \mathbb{K}$ (n fois).
3. Montrer que les $\mathbb{R}$-espaces vectoriels $\mathbb{R}^5$ et $\mathbb{R}^2 \times \mathbb{R}^3$ sont isomorphes.

Définition 1.9 – *Soit E un $\mathbb{K}$-espace vectoriel. On appelle sous-espace vectoriel de E tout sous-ensemble F de E telle que :*
(i) F est un sous-groupe de E ;
(ii) pour tout $\lambda \in \mathbb{K}$ et tout $x \in F$, $\lambda x \in F$ (stabilité de F par produit externe).

Remarque 1.10 – Soient E un $\mathbb{K}$-espace vectoriel et F une sous-espace vectoriel de E. Les restrictions à F des lois de composition qui définissent la structure d'espace vectoriel de E munissent F d'une structure de $\mathbb{K}$-espace vectoriel.

Exercice 1.11 – Soit E un $\mathbb{K}$-espace vectoriel et F un sous-ensemble de E. Montrer que F est un sous-espace vectoriel de E si et seulement si il vérifie les trois propriétés suivantes :
(i) $0 \in F$;
(ii) pour tous $x, y \in F$, $x + y \in F$ (stabilité de F par somme) ;
(iii) pour tout $\lambda \in \mathbb{K}$ et tout $x \in F$, $\lambda x \in F$ (stabilité de F par produit externe).

Exemple 1.12 – Soit $n \in \mathbb{N}$. On note $\mathbb{K}_n[X]$ le sous-ensemble de $\mathbb{K}[X]$ des polynômes dont le degré est inférieur ou égal à n. Alors, $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$.

On introduit maintenant la notion de *combinaison linéaire*. Pour cela, il faut préciser le point pratique suivant. Soit I un ensemble et $(\lambda_i)_{i \in I}$ une famille d'éléments de $\mathbb{K}$. On dit que la famille $(\lambda_i)_{i \in I}$ est presque nulle si le sous-ensemble J de I des éléments i tels que $\lambda_i \neq 0$ est fini.

Définition 1.13 – *Soit E un $\mathbb{K}$-espace vectoriel.*
1. Si I est un ensemble non-vide et $\mathcal{X} = (x_i)_{i \in I}$ une famille indexée par I d'éléments de E. Un élément x de E est dit combinaison linéaire d'éléments de $\mathcal{X}$ si il existe une famille presque nulle $(\lambda_i)_{i \in I}$ d'éléments de $\mathbb{K}$ telle que $x = \sum_{i \in I} \lambda_i x_i$. L'ensemble de tous les vecteurs de E qui sont combinaison linéaire d'éléments de $\mathcal{X}$ est noté $\mathrm{CL}(\mathcal{X})$.
2. Si A est un sous-ensemble non vide de E, un élément x est dit combinaison linéaire d'éléments de A s'il est combinaison linéaire de la famille associée à A. L'ensemble de tous les vecteurs de E qui sont combinaison linéaire d'éléments de A est noté $\mathrm{CL}(A)$.

Remarque 1.14 – Soient E un $\mathbb{K}$-espace vectoriel. Si A est un sous-ensemble non vide de E, un élément x est combinaison linéaire d'éléments de A si et seulement si il existe $n \in \mathbb{N}^*$, $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ et $a_1, \ldots, a_n \in A$ tels que $x = \sum_{1 \leq i \leq n} \lambda_i a_i$.

Remarque 1.15 – Soit E un $\mathbb{K}$-espace vectoriel. Par convention, on pose que l'ensemble des combinaisons linéaires d'une famille indexée par $\emptyset$ est $\{0\}$.

Exercice 1.16 – Soient E un $\mathbb{K}$-espace vectoriel, I un ensemble et $\mathcal{X} = (x_i)_{i\in I}$ une famille indexée par I d'éléments de E. Montrer que $\mathrm{CL}(\mathcal{X})$ est un sous-espace vectoriel de E.

Définition 1.17 – *Soient E, F deux $\mathbb{K}$-espaces vectoriels et $f : E \longrightarrow F$ une application linéaire. On appelle noyau de f le sous-ensemble* $\ker f = f^{-1}(0)$ *de E et image de f le sous-ensemble* $\mathrm{im} f = f(E)$ *de F.*

Exercice 1.18 – Soient E, F deux $\mathbb{K}$-espaces vectoriels et $f : E \longrightarrow F$ une application linéaire. Montrer que l'image $f(U)$ d'un sous-espace vectoriel U de E est un sous-espace vectoriel de F. Montrer que l'image réciproque $f^{-1}(V)$ d'un sous-espace vectoriel V de F est un sous-espace vectoriel de E. En déduire que le noyau et l'image de f sont des sous-espaces vectoriels de E et F, respectivement.

Exercice 1.19 – Soit E un $\mathbb{K}$-espace vectoriel, soit I un ensemble non-vide et soit $(E_i)_{i\in I}$ une famille indexée par I de sous-espaces vectoriels de E. Montrer que l'intersection $\cap_{i\in I} E_i$ des sous-espaces de cette famille est un sous-espace vectoriel de E.

Définition 1.20 – *Soit E un $\mathbb{K}$-espace vectoriel.*
1. Soit A est une partie de E. Le sous-espace vectoriel de E engendré par A est l'intersection de tous les sous-espaces vectoriels de E contenant A ; il est noté $\mathrm{Vect}(A)$.
2. Soit I est un ensemble non-vide et $\mathcal{X} = (x_i)_{i\in I}$ une famille indexée par I d'éléments de E. Le sous-espace vectoriel de E engendré par $\mathcal{X}$ est le sous-espace vectoriel de E engendré par le sous-ensemble de E associé à $\mathcal{X}$.

Exercice 1.21 – Soient E un $\mathbb{K}$-espace vectoriel et A un sous-ensemble de E.
1. Montrer que $\mathrm{Vect}(A) = \mathrm{CL}(A)$.
2. Montrer que tout sous-espace vectoriel de E contenant A contient $\mathrm{Vect}(A)$.

Définition 1.22 – *Soient E un $\mathbb{K}$-espace vectoriel, $n \in \mathbb{N}^*$ et $E_1, \ldots, E_n$ des sous-espaces vectoriels de E. La somme des sous-espaces vectoriels $E_1, \ldots, E_n$ est le sous-espace vectoriel de E engendré par $\cup_{i=1}^n E_i$. Elle est notée $\sum_{i=1}^n E_i$.*

Exercice 1.23 – Soient E un $\mathbb{K}$-espace vectoriel, $n \in \mathbb{N}^*$ et $E_1, \ldots, E_n$ des sous-espaces vectoriels de E. Montrer qu'un élément x de E est dans $\sum_{i=1}^n E_i$ si et seulement si, pour $i \in \{1, \ldots, n\}$, il existe $x_i \in E_i$ tel que $x = x_1 + \ldots + x_n$.

Proposition 1.24 – *Soient E un $\mathbb{K}$-espace vectoriel, $n \in \mathbb{N}^*$ et $E_1, \ldots, E_n$ des sous-espaces vectoriels de E. Les assertions suivantes sont équivalentes :*
(i) pour tout n-uplet $(x_1, \ldots, x_n) \in E_1 \times \ldots \times E_n$, l'égalité $x_1 + \ldots + x_n = 0$ entraine que $x_i = 0$ pour tout $i \in \{1, \ldots, n\}$;
(ii) pour tous n-uplets $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in E_1 \times \ldots \times E_n$, l'égalité $x_1 + \ldots + x_n = y_1 + \ldots + y_n$ entraine que $x_i = y_i$ pour tout $i \in \{1, \ldots, n\}$;
(iii) pour $i \in \{1, \ldots, n\}$, $E_i \cap \sum_{j\in\{1,\ldots,n\}\setminus\{i\}} E_j = \{0\}$.

Démonstration : Exercice (très instructif). ∎

Définition 1.25 – *Soient E un $\mathbb{K}$-espace vectoriel, $n \in \mathbb{N}^*$ et $E_1, \dots, E_n$ des sous-espaces vectoriels de E. Si les conditions de la proposition 1.24 sont vérifiées, on dit que les sous-espaces vectoriels $E_1, \dots, E_n$ sont en somme directe et on note $\oplus_{i\in\mathbb{N}} E_i$ leur somme.*

Définition 1.26 – *Soient E un $\mathbb{K}$-espace vectoriel et F, G des sous-espaces vectoriels de E. On dit que F et G sont supplémentaires si ils sont en somme directe et si $F \oplus G = E$.*

Exercice 1.27 – Soient E un $\mathbb{K}$-espace vectoriel et F, G des sous-espaces vectoriels de E.
1. Montrer que F et G sont supplémentaires si et seulement si, pour tout $x \in E$, il existe un couple $(x_F, x_G) \in F \times G$ et un seul tel que $x = x_F + x_G$.
2. On considère l'application $p : E \longrightarrow E$ qui à tout $x \in E$ associe x_F (avec les notations ci-dessus). Montrer que p est une application linéaire telle que $p \circ p = p$. On dit que p est la projection sur F parallèlement à G.
3. On considère l'application $s : E \longrightarrow E$ qui à tout $x \in E$ associe $x_F - x_G$ (avec les notations ci-dessus). Montrer que s est une application linéaire telle que $s \circ s = \mathrm{id}$. On dit que s est la symétrie par rapport à F, parallèlement à G.

Définition 1.28 – *Soient E un $\mathbb{K}$-espace vectoriel, I un ensemble non-vide et $\mathcal{X} = (x_i)_{i\in I}$ une famille indexée par I d'éléments de E.*
1. On dit que la famille $\mathcal{X}$ est libre si elle satisfait la propriété suivante : pour toute famille presque nulle $(\lambda_i)_{i\in I}$ d'éléments de $\mathbb{K}$, l'égalité $\sum_{i\in I} \lambda_i x_i = 0$ entraîne que $\lambda_i = 0$ pour tout $i \in I$.
2. On dit que $\mathcal{X}$ est une famille génératrice de E si $E = \mathrm{Vect}(\mathcal{X})$.
3. On dit que $\mathcal{X}$ est une base de E si elle est libre et génératrice.

Remarque 1.29 – Soit E un $\mathbb{K}$-espace vectoriel. Par convention, la famille de E indexée par $\emptyset$ est libre. C'est donc une base de $\{0\}$.

Remarque 1.30 – Soient E un $\mathbb{K}$-espace vectoriel, I un ensemble non-vide et $\mathcal{X} = (x_i)_{i\in I}$ une famille indexée par I d'éléments de E. Si $\mathcal{X}$ est libre, alors pour $i, j \in I$ tels que $i \neq j$, on a $x_i \neq x_j$. Ainsi, la famille $\mathcal{X}$ est en fait un sous-ensemble de E.

Exercice 1.31 – Soient E un $\mathbb{K}$-espace vectoriel, I un ensemble non-vide et $\mathcal{X} = (x_i)_{i\in I}$ une famille indexée par I d'éléments de E. Montrer que $\mathcal{X}$ est une base de E si et seulement si, pour tout $x \in E$, il existe une et une seule famille presque nulle $(\lambda_i)_{i\in I}$ indexée par I d'éléments de $\mathbb{K}$ telle que $x = \sum_{i\in I} \lambda_i x_i$. Cette famille est alors appelée la famille des coordonnées de x relativement à $\mathcal{X}$.

Le théorème suivant est d'une importance cruciale. Sa démonstration repose sur le Lemme de Zorn qui est au delà des objectifs de ce cours. Pour cette raison, on admet ce résultat.

Théorème 1.32 *(Existence de bases.) – Tout $\mathbb{K}$-espace vectoriel admet une base.*

Exemple 1.33 – On reprend les notations des Exemples 1.3 et 1.12.
1. La famille (à un élément) (1) est une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}$.
2. Soit $n \in \mathbb{N}^*$. On considère le $\mathbb{K}$-espace vectoriel $\mathbb{K}^n$. Pour $i \in \{1, \dots, n\}$, on note e_i l'élément de $\mathbb{K}^n$ dont toutes les coordonnées sont nulles sauf la i-ème qui vaut 1. Alors, la famille $(e_i)_{i\in\{1,\dots,n\}}$ est une base de $\mathbb{K}^n$. Elle est appelée la *base canonique* de $\mathbb{K}^n$.
3. La famille $(X^i)_{i\in\mathbb{N}}$ est une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}[X]$. Elle est appelée la *base canonique* de $\mathbb{K}[X]$.
4. Soit $n \in \mathbb{N}$. La famille $(X^i)_{i\in\{0,\dots,n\}}$ est une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}_n[X]$. Elle est appelée la *base canonique* de $\mathbb{K}_n[X]$. En particulier, $\mathbb{K}_0[X]$ est l'ensemble des polynômes constants et il admet (1) pour base.

2 Espaces vectoriels de dimension finie.

Définition 2.1 – *On dit qu'un $\mathbb{K}$-espace vectoriel E est de dimension finie si il possède une partie génératrice finie.*

Exercice 2.2 – *Montrer que le $\mathbb{K}$-espace vectoriel $\mathbb{K}[X]$ n'est pas de dimension finie.*

Théorème 2.3 – *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie.*
1. Si X est une partie génératrice finie de E, alors X contient une base de E. En particulier, tout $\mathbb{K}$-espace vectoriel de dimension finie admet une base.
2. Si L est une partie libre de E, alors L est finie et de cardinal majoré par celui de toute partie génératrice de E.
3. Si L est une partie libre de E, il existe une base B de E telle que $L \subseteq B$. (Théorème de la base incomplète.)
4. Toutes les bases de E ont le même cardinal.

Définition 2.4 – *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Le cardinal commun à toutes les bases de E est appelé le dimension de E et est noté* $\dim_{\mathbb{K}}(E)$.

Exemple 2.5 – On reprend les notations et résultats des Exemples 1.3, 1.12 et 1.33.
1. Soit $n \in \mathbb{N}^*$, $\dim_{\mathbb{K}}(\mathbb{K}^n) = n$.
2. Soit $n \in \mathbb{N}$, $\dim_{\mathbb{K}}(\mathbb{K}_n[X]) = n+1$.

Corollaire 2.6 – *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie égale à n.*
*1. Une partie libre de E est une base de E si et seulement si elle est maximale parmi les parties libres (*c-à-d : *elle n'est strictement contenu dans aucune partie libre) si et seulement si elle est de cardinal n.*
*2. Une partie génératrice de E est une base de E si et seulement si elle est minimale parmi les parties génératrices (*c-à-d : *elle ne contient strictement aucune partie génératrice) si et seulement si elle est de cardinal n.*

Corollaire 2.7 – *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Tout sous-espace vectoriel de E admet un supplémentaire.*

Démonstration : Exercice facile et important. ∎

Proposition 2.8 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et F un sous-espace vectoriel de E. Alors, F est un $\mathbb{K}$-espace vectoriel de dimension finie et* $\dim_{\mathbb{K}} F \leq \dim_K E$. *De plus, $F = E$ si et seulement si* $\dim_{\mathbb{K}} F = \dim_{\mathbb{K}} E$.

Définition 2.9 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $\mathcal{X}$ une famille d'éléments de E. On appelle rang de $\mathcal{X}$, que l'on note* $\mathrm{rg}\mathcal{X}$, *la dimension du sous-espace vectoriel de E engendré par $\mathcal{X}$.*

Proposition 2.10 – *Soient E un $\mathbb{K}$-espace vectoriel, $n \in \mathbb{N}^*$ et $E_1, \ldots, E_n$ des sous-espaces vectoriels de E en somme directe. Alors,* $\dim_{\mathbb{K}} \oplus_{i\in\mathbb{N}} E_i = \sum_{i=1}^{n} \dim_{\mathbb{K}} E_i$.

Exercice 2.11 – (Etend le cas $n = 2$ de la proposition 2.10.) Soient E un $\mathbb{K}$-espace vectoriel, et F, G des sous-espaces vectoriels de E. Alors $\dim_{\mathbb{K}}(F+G) = \dim_{\mathbb{K}} F + \dim_K G - \dim_{\mathbb{K}} F \cap G$.

Théorème 2.12 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie égale à $n \in \mathbb{N}^*$ et F un $\mathbb{K}$-espace vectoriel. Soient $B = \{b_1, \ldots, b_n\}$ une base de E et $\{x_1, \ldots, x_n\}$ une famille d'éléments de F. Il existe une application linéaire $f : E \longrightarrow F$ et une seule telle que, pour $1 \leq i \leq n$, $f(b_i) = x_i$.*

Exercice 2.13 – Le théorème 2.12 peut être illustré par l'exemple des applications linéaires de $\mathbb{K}^n$ dans $\mathbb{K}^m$, où $m, n \in \mathbb{N}^*$.
1. Soient $a_{i,j}$, $1 \leq i \leq m$, $1 \leq j \leq n$, mn scalaires. Montrer que l'application

$$\begin{array}{rccc} f & : & \mathbb{K}^n & \longrightarrow & \mathbb{K}^m \\ & & (x_1, \ldots, x_n) & \mapsto & (\sum_{i=1}^m a_{1,i}x_i, \ldots, \sum_{i=1}^m a_{m,i}x_i) \end{array}$$

est linéaire.
2. Soit $f : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ une application linéaire. Montrer qu'il existe une unique famille $(a_{i,j})_{1 \leq i \leq m,\, 1 \leq j \leq n}$ de scalaires telle que

$$\begin{array}{rccc} f & : & \mathbb{K}^n & \longrightarrow & \mathbb{K}^m \\ & & (x_1, \ldots, x_n) & \mapsto & (\sum_{i=1}^m a_{1,i}x_i, \ldots, \sum_{i=1}^m a_{m,i}x_i) \end{array}$$

Proposition 2.14 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie égale à $n \in \mathbb{N}^*$, F un $\mathbb{K}$-espace vectoriel et $f : E \longrightarrow F$ une application linéaire. Si $B = \{b_1, \ldots, b_n\}$ est une famille génératrice de E, alors* $\mathrm{im}f = \mathrm{Vect}\{f(b_1), \ldots, f(b_n)\}$.

Exercice 2.15 – Soient E un $\mathbb{K}$-espace vectoriel de dimension finie égale à $n \in \mathbb{N}^*$, F un $\mathbb{K}$-espace vectoriel et $f : E \longrightarrow F$ une application linéaire. Alors la dimension de $\mathrm{im}(f)$ est finie et majorée par n.

Définition 2.16 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie, F un $\mathbb{K}$-espace vectoriel et $f : E \longrightarrow F$ une application linéaire. Le rang de f, noté* $\mathrm{rg}(f)$*, est la dimension de* $\mathrm{im}f$.

Théorème 2.17 *(Théorème du rang.) – Soient E un $\mathbb{K}$-espace vectoriel de dimension finie, F un $\mathbb{K}$-espace vectoriel et $f : E \longrightarrow F$ une application linéaire. Alors,*

$$\dim_{\mathbb{K}} E = \dim_{\mathbb{K}} \ker(f) + \dim_{\mathbb{K}} \mathrm{im}(f).$$

Théorème 2.18 – *Soient E et F des $\mathbb{K}$-espaces vectoriels de même dimension finie et $f : E \longrightarrow F$ une application linéaire. Les assertions suivantes sont équivalentes :*
(i) f est injective ;
(ii) f est surjective ;
(iii) f est un isomorphisme.

3 Structure d'algèbre.

On introduit dans cette section une structure très utile dans la suite, celle d'*algèbre sur un corps.* Cette structure en mélange deux déjà rencontrées, la structure d'anneau et la structure d'espace vectoriel.

Définition 3.1 – *On appelle algèbre sur le corps $\mathbb{K}$ (ou $\mathbb{K}$-algèbre) un ensemble A muni de deux l.c.i. (notées $+$ et $\times$) et d'une l.c.e. à scalaires dans $\mathbb{K}$ (notée $.$) telles que :*
1. $(A, +, \times)$ soit un anneau ;
2. $(A, +, .)$ soit un $\mathbb{K}$-espace vectoriel ;
3. pour tous $\lambda \in \mathbb{K}$, $a, b \in A$, $\lambda.(a \times b) = (\lambda.a) \times b = a \times (\lambda.b)$.
Un algèbre sur le corps $\mathbb{K}$ est dite commutative si l'anneau sous-jacent l'est.

Remarque 3.2 – Dans la définition 3.1, la troisième condition exprime la nécessité d'une règle de compatibilité entre le produit interne ($\times$) et le produit externe ($.$) d'une algèbre sur un corps. Il résulte en particulier de cette condition que, si I est un sous-ensemble de A qui est un idéal de l'anneau $(A, +, \times)$, alors I est un sous-espace vectoriel pour $(A, +, .)$.

Remarque 3.3 – Soit $(A, +, \times, .)$ une $\mathbb{K}$-algèbre. Il faut prendre garde que l'on est en présence de deux multiplications internes, celle de $\mathbb{K}$ et celle de A. En particulier, on a un neutre pour la multiplication dans $\mathbb{K}$, $1_{\mathbb{K}}$, et un neutre pour la multiplication interne dans A, 1_A. Il résulte de la définition d'espace vectoriel que ces deux neutres vérifient $1_{\mathbb{K}}.1_A = 1_A$.

Définition 3.4 – *Soit A une $\mathbb{K}$-algèbre dont on note $+$, $\times$ et $.$ les lois de composition. Un sous-ensemble B de A est appelé une sous-$\mathbb{K}$-algèbre de A si c'est un sous-anneau de $(A, +, \times)$ et un sous-$\mathbb{K}$-espace vectoriel de $(A, +, .)$.*

Définition 3.5 – *Soient $(A, +, \times, .)$ et $(B, +, \times, .)$ deux $\mathbb{K}$-algèbres. On dit qu'une application $f : A \longrightarrow B$ est un morphisme de $\mathbb{K}$-algèbres si f est un morphisme de $\mathbb{K}$-espaces vectoriels (c'est-à-dire une application linéaire) et un morphisme d'anneaux. Un isomorphisme de $\mathbb{K}$-algèbres est un morphisme bijectif de $\mathbb{K}$-algèbres. Un endomorphisme de $\mathbb{K}$-algèbre est un morphisme d'une $\mathbb{K}$-algèbre vers elle-même. Un automorphisme de $\mathbb{K}$-algèbre est un endomorphisme bijectif d'une $\mathbb{K}$-algèbre vers elle-même.*

Dans la suite du cours, on rencontrera trois exemples d'algèbres sur un corps. On en présente deux pour commencer : l'algèbre des polynômes à coefficients dans un corps et l'algèbre des endomorphismes d'un espace vectoriel. Pour introduire le premier exemple ci-dessus, on doit commencer par un exemple général de construction d'une algèbre.

Exemple 3.6 – **L'algèbre des applications à valeurs dans un corps.** Soit X un ensemble et $\mathbb{K}$ un corps. On note $\mathcal{F}(X, \mathbb{K})$ l'ensemble des applications de X dans $\mathbb{K}$. On considère alors les deux l.c.i.

$$+ \ : \ \mathcal{F}(X,\mathbb{K}) \times \mathcal{F}(X,\mathbb{K}) \longrightarrow \mathcal{F}(X,\mathbb{K}) \quad \text{et} \quad \times \ : \ \mathcal{F}(X,\mathbb{K}) \times \mathcal{F}(X,\mathbb{K}) \longrightarrow \mathcal{F}(X,\mathbb{K})$$

où, pour $f, g \in \mathcal{F}(X, \mathbb{K})$ et $x \in X$, $(f+g)(x) = f(x)+g(x)$ et $(f \times g)(x) = f(x) \times g(x)$ et la l.c.e.

$$. \ : \ \mathbb{K} \times \mathcal{F}(X,\mathbb{K}) \longrightarrow \mathcal{F}(X,\mathbb{K})$$

où, pour $\lambda \in \mathbb{K}$, $f \in \mathcal{F}(X, \mathbb{K})$ et $x \in X$, $(\lambda.f)(x) = \lambda f(x)$. Avec ces notations, $(\mathcal{F}(X, \mathbb{K}), +, \times, .)$ est une $\mathbb{K}$-algèbre commutative.

Exemple 3.7 – **L'algèbre des polynômes sur un corps.** Soit $\mathbb{K}$ un corps.
1. On a défini, au chapitre V, deux lois de composition interne sur l'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$. On a également défini à la section 1 du présent chapitre une loi de composition externe à scalaires dans $\mathbb{K}$ sur $\mathbb{K}[X]$. Muni de ces trois lois de composition, l'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est une $\mathbb{K}$-algèbre commutative.
2. L'application $i_{\mathbb{K}}$ du Lemme 1.4, Chapitre V est un morphisme de $\mathbb{K}$-algèbres.
3. On rappelle les notations de la section 3 du Chapitre V : $\mathcal{F}(\mathbb{K})$ désigne l'ensemble des applications de $\mathbb{K}$ dans $\mathbb{K}$ et $\mathcal{F}_{\text{pol}}(\mathbb{K})$ est le sous-anneau des applications polynomiales de $\mathbb{K}$ dans $\mathbb{K}$. Conformément à l'Exemple 3.6, $\mathcal{F}(\mathbb{K})$ est une $\mathbb{K}$-algèbre et il est facile de vérifier que $\mathcal{F}_{\text{pol}}(X)$ est une sous-$\mathbb{K}$-algèbre de $\mathcal{F}(\mathbb{K})$. De plus, l'application $\mathbb{K}[X] \longrightarrow \mathcal{F}(X)$ du Chapitre V, Remarque 3.1.3 est un morphisme de $\mathbb{K}$-algèbres.

Exemple 3.8 – **L'algèbre des endomorphismes sur un espace vectoriel.** Soit $\mathbb{K}$ un corps et V un $\mathbb{K}$-espace vectoriel. Conformément à l'Exercice 1.7 et en en reprennant les notations, $\mathcal{L}(E)$ est muni d'une addition (notée $+$) et d'un produit externe (noté .) tels quel $(\mathcal{L}(E), +, .)$ soit un $\mathbb{K}$-espace vectoriel. En outre, la composition des applications définie sur $\mathcal{L}(E)$ une autre loi de composition interne, que l'on note $\circ$. On vérifie facilement que $(\mathcal{L}(E), +, \circ, .)$ est une $\mathbb{K}$-algèbre. Attention, en général $\mathcal{L}(E)$ n'est pas commutative. En fait, elle l'est si et seulement si E est de dimension finie égale à 0 ou 1.

4 Dualité

On aborde maintenant l'étude des *formes linéaires.* A ce sujet, on rappelle que le corps $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel, de dimension finie égale à 1.

Définition 4.1 – *Soit E un $\mathbb{K}$-espace vectoriel. On appelle forme linéaire sur E toute application linéaire de E dans $\mathbb{K}$. L'ensemble de toutes les formes linéaires sur E est appelé le dual de E et est noté E^*.*

Remarque 4.2 – Soit E un $\mathbb{K}$-espace vectoriel. Le dual E^* de E est un $\mathbb{K}$-espace vectoriel.

Définition 4.3 – *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$. On appelle hyperplan de E tout sous-espace vectoriel de E de dimension $n-1$.*

Théorème 4.4 – *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$.*
1. Le noyau d'une forme linéaire non nulle sur E est un hyperplan.
2. Si H est un hyperplan de E, il existe une forme linéaire non nulle dont H est le noyau.
3. Deux formes linéaires non nulles ϕ et ψ ont le même noyau si et seulement si il existe $\lambda \in \mathbb{K}$ tel que $\psi = \lambda\phi$.

Démonstration : Le point 1 est une conséquence immédiate du théorème du rang.

Pour le point 2, on peut considérer une base $\{b_1, \ldots, b_{n-1}\}$ de H et la compléter en une base $\{b_1, \ldots, b_n\}$ de E. On sait alors qu'il existe une forme linéaire $\phi : E \longrightarrow \mathbb{K}$ telle que $\phi(b_i) = 0$ pour $1 \leq i \leq n-1$ et $\phi(b_n) = 1$. Il est facile de vérifier que $\ker\phi = H$.

Pour le point 3, il est clair que si il existe $\lambda \in \mathbb{K}$ tel que $\psi = \lambda\phi$ alors ϕ et ψ ont le même noyau. Réciproquement, si ϕ et ψ ont le même noyau H. Comme les formes linéaires ϕ et ψ sont non nulles, H est un hyperplan de E. Cet hyperplan admet un supplémentaire qui est un sous-espace vectoriel de dimension 1 de E. Donc il existe $v \in E \setminus \{0\}$ tel que $E = H \oplus \mathbb{K}v$. Comme ϕ est non nulle, on doit avoir $\phi(v) \neq 0$. Posant $\lambda = \psi(v)/\phi(v)$, on vérifie facilement que $\psi = \lambda\phi$. ∎

Remarque 4.5 –
1. Soient E un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}^*$ et H un hyperplan de E. D'après le théorème 4.4, il existe une forme linéaire non nulle ϕ sur E telle que $H = \ker\phi$. On dit alors que ϕ est une *équation* de H. Le même théorème assure que deux équations de H sont multiples scalaires l'une de l'autre. Par abus de langage, on parle souvent de l'équation de H même si, d'après ce qui précède, une telle équation n'est définie qu'à multiplication près par un scalaire.
2. Le cas du $\mathbb{K}$-espace vectoriel $\mathbb{K}^n$ $(n \in \mathbb{N}^*)$ aide à comprendre le vocabulaire. En effet, soit H un hyperplan de $\mathbb{K}^n$ et ϕ une forme linéaire sur $\mathbb{K}^n$ telle que $\ker\phi = H$. On sait qu'il existe une unique famille $\{a_1, \ldots, a_n\}$ d'éléments de $\mathbb{K}$ telle que

$$\begin{array}{rccc} \phi & : & \mathbb{K}^n & \longrightarrow & \mathbb{K} \\ & & (x_1, \ldots, x_n) & \mapsto & a_1x_1 + \ldots + a_nx_n \end{array}.$$

Ainsi, on a $H = \{(x_1, \ldots, x_n) \in \mathbb{K}^n \,|\, a_1x_1 + \ldots + a_nx_n = 0\}$. Ce qui définit H à l'aide d'une équation (au sens le plus usuel du terme). De plus, si une autre équation permet de définir H de la même façon, cette équation détermine une autre forme linéaire qui, d'après ce qui précède, doit être multiple scalaire de ϕ. On en déduit que cette seconde équation est un multiple de la précédente.

On étudie maintenant plus en détail les relations existant entre un espace vectoriel et son dual.

Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}^*$. Si $\mathcal{B} = \{e_1, \ldots, e_n\}$ est une base de E, on peut définir les formes linéaires $e_1^*, \ldots, e_n^*$ suivantes : pour $1 \leq i \leq n$, e_i^* est définie en posant que, pour $1 \leq j \leq n$, $e_i^*(e_j) = \delta_{ij}$. Ainsi, si x est un élément de E et si $x_1, \ldots, x_n$ sont les coordonnées de x dans la base $\mathcal{B}$, pour $1 \leq i \leq n$, on a $e_i^*(x) = e_i^*(\sum_{j=1}^n x_j e_j) = \sum_{j=1}^n x_j e_i^*(e_j) = x_i$. Pour cette raison, la forme linéaire e_i^*, $1 \leq i \leq n$, est appelée la i-ième forme coordonnée associée à la base $\mathcal{B}$.

Théorème 4.6 – *Avec les notations précédentes, la famille $\{e_1^*, \ldots, e_n^*\}$ est une base de E^*. En particulier,* $\dim_{\mathbb{K}} E^* = \dim_{\mathbb{K}} E$.

Démonstration : Exercice facile et important. ∎

Définition 4.7 – *Avec les notations précédentes, la base $\{e_1^*, \ldots, e_n^*\}$ de E^* est appelée la base duale de la base $\{e_1, \ldots, e_n\}$ de E.*

On passe maintenant à la notion d'orthogonalité.

Définition 4.8 – *Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}^*$.*
1. Si A est une partie de E, l'orthogonal de A dans E^*, noté $A^\perp$, est le sous-ensemble de E^* des formes linéaires qui s'annulent sur tout élément de A.
2. Si A est une partie de E^*, l'orthogonal de A dans E, noté $A^\perp$, est le sous-ensemble de E des eléments dont l'image par tout élément de A est nulle.

Proposition 4.9 – *Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}^*$.*
1. Si A est une partie de E (resp. E^*), $A^\perp$ est un sous-espace vectoriel de E^* (resp. E).
2. Si A et B sont des parties de E (resp. E^*) telles que $A \subseteq B$, alors $A^\perp \supseteq B^\perp$. Si A et B sont des parties de E (resp. E^*), $(A \cup B)^\perp = A^\perp \cap B^\perp$.
3. Si A est une partie de E (resp. E^*), A et $\mathrm{Vect}(A)$ *ont même orthogonal.*
4. Si F est un sous-espace vectoriel de E, alors $F \subseteq (F^\perp)^\perp$.

Théorème 4.10 – *Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}^*$.*
1. Si F est un sous-espace vectoriel de E, alors :

$$\dim_{\mathbb{K}} F + \dim_{\mathbb{K}} F^\perp = \dim_{\mathbb{K}} E.$$

2. On a $(F^\perp)^\perp = F$.

Démonstration : 1. Soit m la dimension de F. On peut considérer une base $\mathcal{B} = \{e_1, \ldots, e_n\}$ de E telle que $\{e_1, \ldots, e_m\}$ soit une base de F. Il n'est pas difficile de vérifier que $\{e_{m+1}^*, \ldots, e_n^*\}$ est une base de $F^\perp$.

Pour montrer 2, il suffit de se souvenir que $F \subseteq (F^\perp)^\perp$ et de comparer les dimensions. ∎

Remarque 4.11 – La notion d'orthogonal précise le fait, bien connu, qu'il y a deux façons de déterminer un sous-espace vectoriel de $\mathbb{K}^n$ ($n \in \mathbb{N}^*$) : l'une par la donnée d'une base, l'autre par celle d'une famille d'équations.
1. Soit F un sous-espace vectoriel de $\mathbb{K}^n$ de dimension m. Si $\{e_1, \ldots, e_m\}$ est une base de F, on peut la compléter en une base $\{e_1, \ldots, e_n\}$ de $\mathbb{K}^n$. La preuve du théorème précédent montre que

$$F^\perp = \mathrm{Vect}\{e_{m+1}^*, \ldots, e_n^*\}.$$

Chacune des formes linéaires e_i^*, pour $m+1 \leq i \leq n$, a pour noyau un hyperplan H_i (auquel correspond une équation donnée par l'expression explicite de e_i^*). On a alors $F = \cap_{i=m+1}^n H_i$. Autrement dit, H est l'ensemble des éléments de F satisfaisant les $n-m$ équations données par $e_{m+1}^*, \ldots, e_n^*$.
2. Réciproquement, soit F un sous-espace de E déterminé par p équations linéaires ($p \in \mathbb{N}^*$). Chaque équation permet de définir une forme linéaire. On extrait de cette famille de p formes linéaires une famille libre (maximale) de m formes linéaires $\phi_1, \ldots, \phi_m$. Soit G le sous-espace vectoriel de E^* engendré par $\phi_1, \ldots, \phi_m$. On peut compléter $\{\phi_1, \ldots, \phi_m\}$ en une base $\{\phi_1, \ldots, \phi_n\}$ de E^*. Soit alors $\{e_1, \ldots, e_n\}$ l'unique base de E dont $\{\phi_1, \ldots, \phi_n\}$ est la base duale. On a $H = \mathrm{Vect}\{e_{m+1}, \ldots, e_n\}$.

On termine cette section par une brève introduction de la transposée d'une application linéaire. Cette notion sera utile dans l'étude pratique des matrices.

Définition 4.12 – *Soient E et F des $\mathbb{K}$-espaces vectoriels et $f : E \longrightarrow F$ une application linéaire. On appelle transposée de f l'application*

$$\begin{array}{rccc} {}^tf & : & F^* & \longrightarrow & E^* \\ & & \lambda & \mapsto & \lambda \circ f \end{array}$$

Le résultat suivant sera utile dans la suite.

Proposition 4.13 – *Soient E et F des $\mathbb{K}$-espaces vectoriels de dimension finie et $f : E \longrightarrow F$ une application linéaire. Alors,*
1. l'application ${}^tf : F^* \longrightarrow E^*$ est linéaire ;
2. $\ker {}^tf = (\mathrm{im} f)^\perp$ *;*
3. $\mathrm{rg}\, {}^tf = \mathrm{rg} f$.

Démonstration : Le premier point est une simple vérification. Le second découle immédiatement de la définition du noyau et de l'orthogonal. Pour le troisième, il faut utiliser le théorème du rang et le théorème 4.10. ∎

5 Matrices.

Dans la suite, si $r \in \mathbb{N}^*$, on pose $\mathbb{N}_r^* = \{1, \ldots, r\}$.

Définition 5.1 – *Soient $m, n \in \mathbb{N}^*$. On appelle matrice à m lignes et n colonnes (ou de format $m \times n$) à coefficients dans $\mathbb{K}$ toute application de $\mathbb{N}_m^* \times \mathbb{N}_n^*$ dans $\mathbb{K}$. On note $M_{m,n}(\mathbb{K})$ l'ensemble des matrices de format $m \times n$. On pose $M_n(\mathbb{K}) = M_{n,n}(\mathbb{K})$.*

Remarque 5.2 – Soient $m, n \in \mathbb{N}^*$ et A une matrice à m lignes et n colonnes. La donnée de A est donc la donnée d'un élément a_{ij} de $\mathbb{K}$ pour tout couple (i, j) d'entiers tels que $1 \leq i \leq m$ et $1 \leq j \leq n$. La notation classique consiste à présenter ces données sous la forme d'un tableau :

$$A = \begin{pmatrix} a_{11} & \dots & \dots & a_{1n} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{m1} & \dots & \dots & a_{mn} \end{pmatrix}$$

où, pour $1 \leq i \leq m$ et $1 \leq j \leq n$, le coefficient a_{ij} figure en i-ième ligne et j-ième colonne. On utilise aussi la notation $A = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$, plus compacte.

On définit maintenant deux opérations sur les matrices de format $m \times n$, $m, n \in \mathbb{N}^*$. La première, appelée addition, est une l.c.i., la seconde est une l.c.e. à scalaires dans $\mathbb{K}$:

$$\begin{array}{rccc} + \ : & M_{m,n}(\mathbb{K}) \times M_{m,n}(\mathbb{K}) & \longrightarrow & M_{m,n}(\mathbb{K}) \\ & ((a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}, (b_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}) & \mapsto & (a_{ij} + b_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}. \end{array},$$

$$\begin{array}{rccc} . \ : & \mathbb{K} \times M_{m,n}(\mathbb{K}) & \longrightarrow & M_{m,n}(\mathbb{K}) \\ & (\lambda, (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}) & \mapsto & (\lambda a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}. \end{array}.$$

Exercice 5.3 – Soient $m, n \in \mathbb{N}^*$.
1. L'ensemble $M_{m,n}(\mathbb{K})$ muni de la l.c.i. et de la l.c.e. ci-dessus est un $\mathbb{K}$-espace vectoriel.
2. Pour chaque couple $(i, j) \in \mathbb{N}_m^* \times \mathbb{N}_n^*$ on note $E_{i,j}$ la matrice dont tous les coefficients son nuls sauf celui d'indice (i, j) qui vaut 1. Cette matrice est appelée la matrice élémentaire d'indice (i, j). La famille $\{E_{i,j}\}_{1 \leq i \leq m, 1 \leq j \leq n}$ est une base du $\mathbb{K}$-espace vectoriel $M_{m,n}(\mathbb{K})$. En particulier, $\dim_{\mathbb{K}} M_{m,n}(\mathbb{K}) = mn$.

Exercice 5.4 – Soient $m, n \in \mathbb{N}^*$. Notons $\{e_i\}_{1 \leq i \leq n}$ et $\{f_i\}_{1 \leq j \leq m}$ les bases canoniques de $\mathbb{K}^n$ et $\mathbb{K}^m$ respectivemement et, pour chaque couple $(i, j) \in \mathbb{N}_m^* \times \mathbb{N}_n^*$, notons $e_{i,j}$ l'application linéaire de $\mathbb{K}^n$ dans $\mathbb{K}^m$ définie, pour $1 \leq k \leq n$ par $e_{i,j}(e_k) = \delta_{kj} e_i$. (On rappelle que, pour $p, q \in \mathbb{N}$, δ_{pq} est le symbole de Kronecker, qui vaut 1 si $p = q$ et 0 sinon.)
1. Montrer que l'application

$$\begin{array}{rccc} \iota_{m,n} \ : & M_{m,n}(\mathbb{K}) & \longrightarrow & \mathcal{L}(\mathbb{K}^n, \mathbb{K}^m) \\ & E_{i,j} & \mapsto & e_{i,j}. \end{array}$$

est un isomorphisme de $\mathbb{K}$-espaces vectoriels.
2. Décrire explicitement l'application $e_{i,j}$ pour $1 \leq i \leq m$ et $1 \leq j \leq n$.

Définition 5.5 – *Soient $m, n \in \mathbb{N}^*$. La transposée d'une matrice $A = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n} \in M_{m,n}(\mathbb{K})$ est la matrice $B = (b_{ij})_{1 \leq i \leq n, 1 \leq j \leq m} \in M_{n,m}(\mathbb{K})$ définie, pour $1 \leq i \leq n$ et $1 \leq j \leq m$, par $b_{ij} = a_{ji}$. La transposée de la matrice A est notée ${}^tA$.*

Exercice 5.6 – Soient $m, n \in \mathbb{K}$. Montrer que l'application

$$\begin{array}{ccc} M_{m,n}(\mathbb{K}) & \longrightarrow & M_{n,m}(\mathbb{K}) \\ A & \mapsto & {}^tA \end{array}$$

est un isomorphisme de $\mathbb{K}$-espaces vectoriels.

Soient $m, n, p \in \mathbb{N}^*$. Si $A = (a_{ij})_{1\leq i\leq m, 1\leq j\leq n}$ est une matrice de format $m \times n$ et $B = (b_{kl})_{1\leq k\leq n, 1\leq l\leq p}$ une matrice de format $n \times p$, on définit le produit de A et B, noté AB, par $AB = (c_{ij})_{1\leq i\leq m, 1\leq j\leq p} \in M_{m,p}(\mathbb{K})$ où, pour $1 \leq i \leq m, 1 \leq j \leq p$, on pose

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Il est facile de vérifier que le produit ainsi défini vérifie les propriétés usuelles (distributivité à gauche et à droite, associativité, *etc*). Les détails sont laissés au lecteur.

Exercice 5.7 –
1. Calculer le produit de deux matrices élémentaires (de formats compatibles).
2. Soient $m, n, p \in \mathbb{N}^*$, $A \in M_{m,n}(\mathbb{K})$ et $B \in M_{n,p}(\mathbb{K})$. Montrer que ${}^t(AB) = {}^tB\,{}^tA$.

Soit $n \in \mathbb{N}^*$. L'ensemble des matrices carrées de format $n \times n$ est particulièrement intéressant. Pour une telle matrice, les coefficients dont les indices de ligne et colonne coïncident sont appelés diagonaux.

Le produit de matrices permet de définir sur $M_n(\mathbb{K})$ une l.c.i.

$$\begin{array}{rccc} \times & : & M_n(\mathbb{K}) \times M_n(\mathbb{K}) & \longrightarrow & M_n(\mathbb{K}) \\ & & (A, B) & \mapsto & AB. \end{array}$$

Exercice 5.8 – Soit $n \in \mathbb{N}^*$. Muni des opérations d'addition, produit externe et produit interne définis ci-dessus, l'ensemble $M_n(\mathbb{K})$ est une $\mathbb{K}$-algèbre. L'unité pour la multiplication est la matrice, notée I_n, dont tous les coefficients sont nuls sauf les coefficients diagonaux qui valent 1.

Si $n \geq 2$, cette $\mathbb{K}$-algèbre n'est ni commutative, ni intègre.

Compte tenu de ce qui précède, pour $n \in \mathbb{N}^*$, $M_n(\mathbb{K})$ est en particulier un anneau. On dispose donc de la notion de matrice inversible. Le sous-ensemble de $M_n(\mathbb{K})$ formé des matrices inversibles est donc un groupe pour le produit. Ce groupe est noté $GL_n(\mathbb{K})$ et est appelé le groupe général linéaire d'ordre n sur $\mathbb{K}$.

Exercice 5.9 – Soit $n \in \mathbb{N}^*$.
1. Les matrices élémentaires de $M_n(\mathbb{K})$ sont-elles inversibles ?
2. Soit $A \in M_n(\mathbb{K})$. Alors, A est inversible si et seulement si ${}^tA$ est inversible.

Définition 5.10 – *Soient $n \in \mathbb{N}^*$ et $A = (a_{ij})_{1\leq i,j\leq n} \in M_n(\mathbb{K})$.*
1. On dit que A est diagonale si, pour $1 \leq i, j \leq n$, on a $a_{ij} = 0$ lorsque $i \neq j$.
2. On dit que A est triangulaire supérieure (resp. inférieur) si, pour $1 \leq i, j \leq n$, on a $a_{ij} = 0$ lorsque $i > j$ (resp. $i < j$).
3. On dit que A est triangulaire supérieure (resp. inférieur) stricte si, pour $1 \leq i, j \leq n$, on a $a_{ij} = 0$ lorsque $i \geq j$ (resp. $i \leq j$).
4. On dit que A est symétrique si, pour $1 \leq i, j \leq n$, on a $a_{ij} = a_{ji}$.
5. On dit que A est antisymétrique si, pour $1 \leq i, j \leq n$, on a $a_{ij} = -a_{ji}$.

Exercice 5.11 – Soit $n \in \mathbb{N}^*$.
1. Montrer que l'ensemble, noté $S_n(\mathbb{K})$, des matrices symétriques est un sous-espace vectoriel de $M_n(\mathbb{K})$. En donner une base (en utilisant les matrices élémentaires.)
2. Montrer que l'ensemble, noté $A_n(\mathbb{K})$, des matrices antisymétriques est un sous-espace vectoriel de $M_n(\mathbb{K})$. En donner une base (en utilisant les matrices élémentaires.)
3. Montrer que $S_n(\mathbb{K})$ et $A_n(\mathbb{K})$ sont supplémentaires dans $M_n(\mathbb{K})$.

On s'interesse maintenant au lien entre matrices et applications linéaires en dimensions finies.

Définition 5.12 – *Soient E, F deux $\mathbb{K}$-espaces vectoriels de dimension finie non nulle, respectivement égales à n et m et $f : E \longrightarrow F$ une application linéaire. Soient en outre $\mathcal{E} = \{e_1, \ldots, e_n\}$ une base de de E et $\mathcal{F} = \{f_1, \ldots, f_m\}$ une base de $\mathcal{F}$. La matrice représentative de l'application linéaire f dans les bases $\mathcal{E}$ et $\mathcal{F}$ est la matrice $(a_{ij})_{1\leq i\leq m, 1\leq j\leq n}$ dont les coefficients sont définis par :*

$$f(e_j) = \sum_{i=1}^{m} a_{ij} f_i, \quad \textit{pour} \quad 1 \leq j \leq n.$$

On la note $\mathrm{Mat}_{\mathcal{E},\mathcal{F}}(f)$. *Lorsque $E = F$ et $\mathcal{E} = \mathcal{F}$, la matrice représentative de f dans les bases $\mathcal{E}$ et $\mathcal{E}$ est appelée la matrice représentative de f dans la base $\mathcal{E}$ et est notée* $\mathrm{Mat}_{\mathcal{E}}(f)$.

Remarque 5.13 – On reprend les notations de la definition 5.12. Soit $x = x_1e_1 + \ldots + x_ne_n \in E$. Si $y = y_1f_1 + \ldots + y_mf_m$ est l'image de x par f, on a

$$y_i = \sum_{j=1}^{n} a_{ij} x_j, \quad \text{pour} \quad 1 \leq i \leq m.$$

Exercice 5.14 – Soient E, F deux $\mathbb{K}$-espaces vectoriels de dimension finie non nulle et $\mathcal{E}$, $\mathcal{F}$ des bases de E et F, respectivement. Montrer que l'application

$$\begin{array}{rccc} \mathrm{Mat}_{\mathcal{E},\mathcal{F}} & : & \mathcal{L}_K(E,F) & \longrightarrow & M_{m,n}(\mathbb{K}) \\ & & f & \mapsto & \mathrm{Mat}_{\mathcal{E},\mathcal{F}}(f) \end{array}$$

est un isomorphisme d'espaces vectoriels.

Exercice 5.15 – Soient E, F deux $\mathbb{K}$-espaces vectoriels de dimension finie non nulle, $\mathcal{E}$ une base de E, $\mathcal{F}$ une base de F et $f : E \longrightarrow F$ une application linéaire. Si $\mathcal{E}^*$ et $\mathcal{F}^*$ désignent les bases duales de $\mathcal{E}$ et $\mathcal{F}$ respectivement, alors on a :

$$\mathrm{Mat}_{\mathcal{F}^*,\mathcal{E}^*}({}^tf) = {}^t\mathrm{Mat}_{\mathcal{E},\mathcal{F}}(f).$$

On passe à la notion de matrice représentative d'un vecteur (ou d'une famille finie de vecteurs) dans une base donnée.

Définition 5.16 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle, égale à n et $\mathcal{E} = \{e_1, \ldots, e_n\}$ une base de E. Si $\{x_1, \ldots, x_p\}$ est une famille de vecteurs de E, on appelle matrice représentative de la famille $\{x_1, \ldots, x_p\}$ dans la base $\mathcal{E}$ la matrice $(a_{ij})_{1\leq i\leq n, 1\leq j\leq p} \in M_{n,p}(\mathbb{K})$, dont les coefficients sont définis par :*

$$x_j = \sum_{i=1}^{n} a_{ij} e_i, \quad \textit{pour} \quad 1 \leq j \leq p.$$

On la note $\mathrm{Mat}_{\mathcal{E}}(x_1, \ldots, x_p)$.

Remarque 5.17 – Avec les notations de la définition 5.12, on a donc

$$\mathrm{Mat}_{\mathcal{E},\mathcal{F}}(f) = \mathrm{Mat}_{\mathcal{F}}(f(e_1), \ldots, f(e_n)).$$

Proposition 5.18 – *Soient E, F deux $\mathbb{K}$-espaces vectoriels de dimension finie non nulle, respectivement égales à n et m, $f : E \longrightarrow F$ une application linéaire, $\mathcal{E} = \{e_1, \ldots, e_n\}$ une base de E et $\mathcal{F} = \{f_1, \ldots, f_m\}$ une base de $\mathcal{F}$. Pour tout $x \in E$,*

$$\mathrm{Mat}_{\mathcal{F}}(f(x)) = \mathrm{Mat}_{\mathcal{E},\mathcal{F}}(f)\mathrm{Mat}_{\mathcal{E}}(x).$$

Proposition 5.19 – *Soient E, F, G trois $\mathbb{K}$-espaces vectoriels de dimension finie non nulle, $f : E \longrightarrow F$, $g : F \longrightarrow G$ des applications linéaires, $\mathcal{E}$ une base de E, $\mathcal{F}$ une base de F et $\mathcal{G}$ une base de G. Alors,*

$$\mathrm{Mat}_{\mathcal{E},\mathcal{G}}(g \circ f) = \mathrm{Mat}_{\mathcal{F},\mathcal{G}}(g)\mathrm{Mat}_{\mathcal{E},\mathcal{F}}(f).$$

Démonstration : Exercice. ∎

Exercice 5.20 – Soient E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle, égal à n et $\mathcal{E}$ une base de E.
1. Montrer que l'application

$$\begin{array}{rccc} \mathrm{Mat}_{\mathcal{E}} & : & \mathcal{L}_K(E) & \longrightarrow & M_n(\mathbb{K}) \\ & & f & \mapsto & \mathrm{Mat}_{\mathcal{E}}(f) \end{array}$$

est un isomorphisme de $\mathbb{K}$-algèbres.
2. Montrer que l'application $\mathrm{Mat}_{\mathcal{E}}$ induit par restriction un isomorphisme de groupes :

$$\begin{array}{ccc} GL_{\mathbb{K}}(E) & \longrightarrow & GL_n(\mathbb{K}) \\ f & \mapsto & \mathrm{Mat}_{\mathcal{E}}(f) \end{array}.$$

Il est clair que la matrice associée à une application linéaire ou à une famille de vecteurs dépend de façon cruciale du choix des bases de référence. On fait maintenant le lien entre les matrices obtenues pour des choix de bases différents. La clef est la notion de matrice de passage.

Définition 5.21 – *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle, égal à n. Soient en outre $\mathcal{E} = \{e_1, \ldots, e_n\}$ et $\mathcal{E}' = \{e'_1, \ldots, e'_n\}$ des bases de E. La matrice de passage de $\mathcal{E}$ à $\mathcal{E}'$, notée $P_{\mathcal{E},\mathcal{E}'}$, est définie par :*

$$P_{\mathcal{E},\mathcal{E}'} = \mathrm{Mat}_{\mathcal{E}}(e'_1, \ldots, e'_n).$$

Pour démontrer les résultats que nous énonçons ci-dessous, il est commode d'interpréter une matrice de passage comme matrice d'un endomorphisme. C'est l'objet de l'exercice suivant.

Exercice 5.22 – Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle, égal à n. Soient en outre $\mathcal{E} = \{e_1, \ldots, e_n\}$ et $\mathcal{E}' = \{e'_1, \ldots, e'_n\}$ des bases de E. La matrice de passage de $\mathcal{E}$ à $\mathcal{E}'$ est la matrice représentative de l'application identité de E dans les bases $\mathcal{E}'$ et $\mathcal{E}$:

$$P_{\mathcal{E},\mathcal{E}'} = \mathrm{Mat}_{\mathcal{E}',\mathcal{E}}(\mathrm{id}_E).$$

Proposition 5.23 – *Soient E un espace vectoriel de dimension finie et non nulle. Soient $\mathcal{E}, \mathcal{E}', \mathcal{E}''$ des bases de E. On a les résultats suivants ;*
1. la matrice $P_{\mathcal{E},\mathcal{E}'}$ est inversible et son inverse est $P_{\mathcal{E}',\mathcal{E}}$;
2. pour tout vecteur x de E,

$$\mathrm{Mat}_{\mathcal{E}}(x) = P_{\mathcal{E},\mathcal{E}'}\mathrm{Mat}_{\mathcal{E}'}(x) \ ;$$

3. $P_{\mathcal{E},\mathcal{E}''} = P_{\mathcal{E},\mathcal{E}'}P_{\mathcal{E}',\mathcal{E}''}$.

Démonstration : On peut procéder par calcul explicite en revenant aux définitions. Mais c'est fastidieux. Une autre approche consiste à utiliser systématiquement le résultat de l'exercice 5.22. Par exemple, le troisième point se déduit immédiatement de la proposition 5.19 via l'exercice 5.22. ∎

Proposition 5.24 – *Soient E, F des espaces vectoriels de dimension finie et non nulle. Soient $\mathcal{E}, \mathcal{E}'$ deux bases de E, $\mathcal{F}, \mathcal{F}'$ deux bases de F et $\mathcal{G}, \mathcal{G}'$ deux bases de G. Alors,*

$$\mathrm{Mat}_{\mathcal{E}',\mathcal{F}'}(f) = P^{-1}_{\mathcal{F},\mathcal{F}'}\mathrm{Mat}_{\mathcal{E},\mathcal{F}}(f)P_{\mathcal{E},\mathcal{E}'}.$$

Démonstration : Même commentaire que pour la proposition 5.23. ∎

Corollaire 5.25 – *Soient E un espace vectoriel de dimension finie et non nulle et $\mathcal{E}, \mathcal{E}'$ deux bases de E. Alors,*

$$\mathrm{Mat}_{\mathcal{E}'}(f) = P^{-1}_{\mathcal{E},\mathcal{E}'}\mathrm{Mat}_{\mathcal{E}}(f)P_{\mathcal{E},\mathcal{E}'}.$$

On s'intéresse maintenant à deux scalaires que l'on peut attacher à une matrice, sa trace et son rang.

Définition 5.26 – *Soit $n \in \mathbb{N}^*$ et $A = (a_{ij})_{1\leq i,j\leq n} \in M_n(\mathbb{K})$. La trace de A, notée $\mathrm{Tr}(A)$, est définie par*

$$\mathrm{Tr}(A) = \sum_{i=1}^{n} a_{ii}.$$

Exercice 5.27 – Soit $n \in \mathbb{N}^*$.
1. L'application $\mathrm{Tr} : M_n(\mathbb{K}) \mapsto \mathbb{K}$, $A \mapsto \mathrm{Tr}(A)$ est linéaire.
2. Pour $A, B \in M_n(\mathbb{K})$, on a $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

Il résulte de l'exercice 5.27 que, si A et P sont des matrices $n \times n$ ($n \in \mathbb{N}^*$) avec P inversible, on a $\mathrm{Tr}(P^{-1}AP) = \mathrm{Tr}(A)$. On peut donc, en vertue du corollaire 5.25, poser la définition suivante.

Définition 5.28 – *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et non nulle. Si $f \in \mathcal{L}(E)$, on définit la trace de f, notée $Tr(f)$ comme la trace de la matrice représentative de f dans une base de E choisie arbitrairement.*

On passe maintenant à la notion de rang d'une matrice. On va définir le rang d'une matrice à l'aide de la notion de rang d'une application linéaire, introduite plus haut. Pour cela, on commence par une remarque très importante.

Remarque 5.29 – Soient $m, n \in \mathbb{N}^*$ et $A = (a_{ij})_{1\leq i\leq m,1\leq j\leq n} \in M_{m,n}(\mathbb{K})$. Choisissons arbitrairement, d'une part, un espace vectoriel E de dimension n, une base $\mathcal{E}$ de E et, d'autre part, un espace vectoriel F de dimension m et une base $\mathcal{F}$ de F. Il découle du théorème 2.12 qu'il existe une application linéaire $f : E \longrightarrow F$ et une seule telle que,

$$\mathrm{Mat}_{\mathcal{E},\mathcal{F}}(f) = A.$$

On a alors le théorème suivant.

Théorème 5.30 – *On reprend les notations de la remarque 5.29. Si f et g sont deux applications linéaires obtenues pour des choix (éventuellement) différents de E, F, $\mathcal{E}$ et $\mathcal{F}$, alors f et g ont même rang.*

On peut donc poser la définition suivante.

Définition 5.31 – *Soient $m, n \in \mathbb{N}^*$ et $A = (a_{ij})_{1\leq i\leq m, 1\leq j\leq n} \in M_{m,n}(\mathbb{K})$. Le rang de A, noté* $\mathrm{rg}(A)$*, est le rang de l'application linéaire associé comme dans la remarque 5.29 à un choix arbitraire de E, F, $\mathcal{E}$ et $\mathcal{F}$.*

Remarque 5.32 –
1. Il découle immédiatement de la définition que le rang d'une matrice de format $m\times n$ ($m, n \in \mathbb{N}^*$) est majoré par m et n.
2. Il découle immédiatement de la proposition 4.13 et du résultat de l'exercice 5.15 qu'une matrice et sa transposée ont le même rang.
3. Dans la pratique, lorsqu'on veut calculer le rang d'une matrice $A = (a_{ij})_{1\leq i\leq m, 1\leq j\leq n} \in M_{m,n}(\mathbb{K})$, on considère le plus souvent les espaces vectoriels $E = \mathbb{K}^n$, $F = \mathbb{K}^m$ et leurs bases canoniques.

Le critère suivant peut s'avérer utile pour calculer le rang d'une matrice. Il utilise les notions de matrice extraite et de matrice bordante d'une matrice extraite que l'on rappelle maintenant.

Définition 5.33 – *Soient $m, n \in \mathbb{N}^*$ et $A = (a_{ij})_{1\leq i\leq m, 1\leq j\leq n} \in M_{m,n}(\mathbb{K})$. Considérons deux entiers $1 \leq p \leq m$, $1 \leq q \leq n$ et p entiers $1 \leq i_1 < \ldots < i_p \leq m$ ainsi que q entiers $1 \leq j_1 < \ldots < j_q \leq n$. La matrice extraite de A correspondant au choix des entiers $1 \leq i_1 < \ldots < i_p \leq m$ et $1 \leq j_1 < \ldots < j_q \leq n$ est la matrice de format $p \times q$ dont le coefficient de ligne α et de colonne β est a_{i_α, j_β}.*

Plus concrètement, la définition 5.33 signifie que la matrice extraite correspondant au choix de p lignes et q colonnes de A est celle obtenue en effaçant les autres lignes et colonnes de A.

Définition 5.34 – *Soient $m, n \in \mathbb{N}^*$ et $A = (a_{ij})_{1\leq i\leq m, 1\leq j\leq n} \in M_{m,n}(\mathbb{K})$. Si B est une matrice extraite de A, carrée de format $r \times r$ ($r \leq \min\{m, n\}$), on appelle matrice bordante de B toute matrice extraite de A, de format $(r + 1) \times (r + 1)$ dont B soit une matrice extraite.*

On a alors le théorème suivant.

Théorème 5.35 – *Soient $m, n \in \mathbb{N}^*$, $A = (a_{ij})_{1\leq i\leq m, 1\leq j\leq n} \in M_{m,n}(\mathbb{K})$ non nulle et r un entier tel que $1 \leq r \leq \min\{m, n\}$. Les assertions suivantes sont équivalentes :*
(i) $\mathrm{rg}(A) = r$ *;*
(ii) il existe une matrice carrée inversible $r \times r$ extraite de A dont toutes les matrices bordantes sont non inversibles.

Corollaire 5.36 – *Soient $m, n \in \mathbb{N}^*$ et $A = (a_{ij})_{1\leq i\leq m, 1\leq j\leq n} \in M_{m,n}(\mathbb{K})$ non nulle. Le rang de A est le plus grand entier r compris entre 1 et $\min\{m, n\}$ tel qu'il existe une matrice carrée de format $r \times r$ extraite de A qui soit inversible.*

On poursuit avec les notions de matrices équivalentes et de matrices semblables.

Définition 5.37 –
1. Soient $m, n \in \mathbb{N}^*$. Deux matrices A et B de format $m \times n$ sont dites équivalentes si il existe une matrice $Q \in GL_m(\mathbb{K})$ et une matrice $P \in GL_n(\mathbb{K})$ telles que $B = QAP$.
2. Soient $n \in \mathbb{N}^*$. Deux matrices A et B de format $n \times n$ sont dites semblables si il existe une matrice $P \in GL_n(\mathbb{K})$ telle que $B = P^{-1}AP$.

Exercice 5.38 – *Soient $m, n \in \mathbb{N}^*$. La relation $\sim$ définie sur $M_{m,n}(\mathbb{K})$ par $A \sim B$ si et seulement si A et B sont des matrices équivalentes est une relation d'équivalence sur $M_{m,n}(\mathbb{K})$.*

Le théorème suivant est très important.

Théorème 5.39 – *Soient $m, n \in \mathbb{N}^*$.*
1. Soit $A = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n} \in M_{m,n}(\mathbb{K})$. La matrice A est de rang $r \in \mathbb{N}^*$ si et seulement si elle est équivalente à la matrice suivante

$$\begin{pmatrix} 1 & 0 & \dots & \dots & 0 & 0 & \dots & \dots & 0 \\ 0 & 1 & \dots & \dots & 0 & 0 & \dots & \dots & 0 \\ \vdots & & & & \vdots & \vdots & & & \vdots \\ 0 & 0 & \dots & \dots & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & \dots & \dots & 0 & 0 & \dots & \dots & 0 \\ \vdots & & & & \vdots & \vdots & & & \vdots \\ 0 & 0 & \dots & \dots & 0 & 0 & \dots & \dots & 0 \end{pmatrix}$$

dont tous les coefficients sont nuls sauf ceux situés sur la i-ième ligne et la i-ième colonne pour $1 \leq i \leq r$.
2. Deux matrices de $M_{m,n}(\mathbb{K})$ sont équivalentes si et seulement si elles ont même rang.

On aborde, enfin, la résolution des systèmes linéaires.

Soient $m, n \in \mathbb{N}^*$. Un système à m équations et n inconnues est la donnée d'un couple (A, b) de matrices, où $A \in M_{m,n}(\mathbb{K})$ et $b \in M_{m,1}(\mathbb{K})$. Posons $A = (a_{ij})$ et $b = (b_i)$. Résoudre ce système c'est déterminer tous les éléments $(x_1, \dots, x_n) \in \mathbb{K}^n$ satisfaisant les m relations suivantes :

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + \dots + a_{2n}x_n &= b_2 \\ \vdots & \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n &= b_m \end{cases}$$

Soit $f : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ l'application linéaire dont la matrice représentative dans les bases canoniques de $\mathbb{K}^m$ et $\mathbb{K}^n$ est A. Il est clair que l'ensemble des solutions du système ci-dessus est le sous-ensemble $f^{-1}(\{(b_1, \dots, b_m)\})$ (ensemble des antécédents par f de $(b_1, \dots, b_m)$). Ainsi, l'ensemble des solutions est de l'un des type suivant :
1. vide ; c'est le cas où $(b_1, \dots, b_m) \notin \mathrm{im} f$;
2. singleton ; c'est le cas où $(b_1, \dots, b_m) \in \mathrm{im} f$ et f est injective ;
3. infini ; c'est le cas où $(b_1, \dots, b_m) \in \mathrm{im} f$ et f n'est pas injective.

Définition 5.40 – *Un système est dit compatible si l'ensemble de ses solutions est non vide.*

On dit que le système est homogène lorque la matrice b est nulle. Dans ces conditions, il est clair que l'ensemble des solutions du système n'est autre que le noyau de f.

Définition 5.41 – *Soit $S = (A, b)$ un système. On appelle rang du système S celui de la matrice A.*

On commence par un cas particulièrement simple.

Définition 5.42 – *Soit $S = (A, b)$ un système à m équations n inconnues. On dit que S est un système de Cramer si $m = n$ et si A est inversible.*

Il est clair alors qu'on a le résultat suivant.

Théorème 5.43 – *Un système de Cramer admet une solution et une seule.*

Lorsqu'on souhaite résoudre un système, deux questions se posent. La première est l'existence de solutions, la seconde est leur détermination. Une notion clé est alors celle de sous-système d'équations principales.

Soit $S = (A, b)$ un système de m équations linéaires à n inconnues. Si $r \in \mathbb{N}^*$ est le rang de ce système, il existe une matrice extraite de A, carrée et inversible de format $r \times r$. Quitte à renuméroter les équations et les inconnues, on peut supposer que la matrice extraite

$$\begin{pmatrix} a_{11} & \dots & a_{1r} \\ a_{21} & \dots & a_{2r} \\ \vdots & & \vdots \\ a_{r1} & \dots & a_{rr} \end{pmatrix}$$

est inversible. Dans ces conditions, les r premières équations et les r premières inconnues de S sont dites *principales*.

On a alors les deux résultats suivants qui résolvent (du moins théoriquement) les problèmes d'existence et de détermination des solutions du système considéré.

Théorème 5.44 – *On reprend les notations ci-dessus. Le système S admet des solutions si et seulement si les $m - r$ matrices suivantes sont non inversibles :*

$$\begin{pmatrix} a_{1,1} & \dots & a_{1,r} & b_1 \\ a_{2,1} & \dots & a_{2,r} & b_2 \\ \vdots & & \vdots & \vdots \\ a_{r,1} & \dots & a_{r,r} & b_r \\ a_{k,1} & \dots & a_{k,r} & b_k \end{pmatrix}$$

où $r + 1 \leq k \leq m$.

Le résultat suivant est souvent appelé théorème de Rouché-Fontené.

Théorème 5.45 – *On reprend les notations ci-dessus. Si le système S admet des solutions, l'ensemble de ses solutions coïncide avec l'ensemble des solutions du sous-système de ses r premières équations (équations principales). Pour résoudre ce sous-système, on donne des valeurs arbitraire aux inconnues non principales et les inconnues principales sont alors déterminées par un système de Cramer.*

6 Applications multilinéaires, déterminants.

On commence par de brefs rappels sur le groupe symétrique. Soit $n \in \mathbb{N}^*$. On note $\mathfrak{S}_n$ le groupe symétrique de degré n. Rappelons que, si $\sigma \in \mathfrak{S}_n$, on note $\varepsilon(\sigma)$ la signature de σ. Il s'agit du nombre défini par :

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

L'application $\varepsilon : \mathfrak{S}_n \longrightarrow \{-1, 1\}$, $\sigma \mapsto \varepsilon(\sigma)$ ainsi définie est un morphisme de groupes.

On introduire maintenant la notion d'application multilinéaire.

Définition 6.1 – *Soit $p \in \mathbb{N}^*$. Soient $E_1, \ldots, E_p, F$ des $\mathbb{K}$-espaces vectoriels.*
1. Une application $\phi : E_1 \times \ldots \times E_p \longrightarrow F$ est dite p-linéaire si, pour tout indice $i \in \{1, \ldots, p\}$ et tous $x_j \in E_j$, $j \in \{1, \ldots, p\}\backslash\{i\}$, l'application partielle $E_i \longrightarrow F$, $x \mapsto \phi(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_p)$ est linéaire.
2. Une forme p-linéaire est une application p-linéaire $\phi : E_1 \times \ldots \times E_p \longrightarrow \mathbb{K}$.

Remarque 6.2 – Soit $p \in \mathbb{N}^*$. Soient $E_1, \ldots, E_p, F$ des $\mathbb{K}$-espaces vectoriels.
Il découle immédiatement de la définition que si $\phi : E_1 \times \ldots \times E_p \longrightarrow F$ est une forme p-linéaire, alors pour tout p-uple $(a_1, \ldots, a_p) \in E_1 \times \ldots \times E_p$ dont l'un des vecteurs a_i est nul, on a $\phi(a_1, \ldots, a_p) = 0$.

On se concentre maintenant sur le cas où, dans les notations ci-dessus, $E_1 = E_2 = \ldots = E_p$ et $F = \mathbb{K}$.

Définition 6.3 – *Soient $p \in \mathbb{N}^*$ et E un $\mathbb{K}$-espace vectoriel. Une forme p-linéaire sur E est une application*

$$\phi \ : \ \overbrace{E \times \ldots \times E}^{p\text{-}fois} \ \longrightarrow \ \mathbb{K}$$

p-linéaire.

Soient $p \in \mathbb{N}^*$, E un $\mathbb{K}$-espace vectoriel et $\phi : E \times \ldots \times E \longrightarrow \mathbb{K}$ une forme p-linéaire sur E. Si σ est une permutation on considère l'application p-linéaire

$$\sigma^*(\phi) : E \times \ldots \times E \longrightarrow F$$

définie de la façon suivante. Pour $(x_1, \ldots, x_p) \in E \times \ldots \times E$, $\sigma^*(\phi)(x_1, \ldots, x_p) = \phi(x_{\sigma(1)}, \ldots, x_{\sigma(p)})$. On remarquera que, pour $\tau, \sigma \in \mathfrak{S}_p$, on a $(\tau\sigma)^*(\phi) = \tau^*(\sigma^*(\phi))$.

Avec ces notations, on pose la définition suivante.

Définition 6.4 – *Soient $p \in \mathbb{N}^*$, E un $\mathbb{K}$-espace vectoriel et $\phi : E \times \ldots \times E \longrightarrow \mathbb{K}$ une forme p-linéaire sur E.*
1. On dit que ϕ est symétrique si, pour tout $\sigma \in \mathfrak{S}_p$, $\sigma^*(\phi) = \phi$.
2. On dit que ϕ est antisymétrique si, pour tout $\sigma \in \mathfrak{S}_p$, $\sigma^*(\phi) = \varepsilon(\sigma)\phi$.
3. On dit que ϕ est alternée si $\phi(x_1, \ldots, x_p) = 0$ pour tout p-uple $(x_1, \ldots, x_p) \in E \times \ldots \times E$ tel que les $x_1, \ldots, x_p$ ne soient pas deux-à-deux distincts.

Exercice 6.5 – Soit $p \in \mathbb{N}^*$ et E un $\mathbb{K}$-espace vectoriel. Si ϕ est une forme p-linéaire alternée sur E et si $(a_1, \ldots, a_p)$ est une famille liée de vecteurs de E, alors $\phi(a_1, \ldots, a_p) = 0$.

La proposition suivante donne une caractérisation utile des formes p-linéaires alternées. Elle a des conséquences pratiques dans le calcul des déterminants.

Proposition 6.6 – *Soient $p \in \mathbb{N}^*$, E un $\mathbb{K}$-espace vectoriel et ϕ une forme p-linéaire sur E. Les assertions suivantes sont équivalentes :*
(i) ϕ est alternée ;
(ii) pour toute transposition τ de $\mathfrak{S}_p$, on a $\tau^*(\phi) = -\phi$;
(iii) pour toute permutation σ de $\mathfrak{S}_p$, on a $\sigma^*(\phi) = \varepsilon(\sigma)\phi$.

Démonstration : Exercice. On pourra utiliser le fait que le groupe symétrique est engendré par l'ensemble des transpositions. ∎

Remarque 6.7 – Soient $p \in \mathbb{N}^*$ et E un $\mathbb{K}$-espace vectoriel. On note $\bigwedge_p^*(E)$ l'ensemble des formes p-linéaires alternées sur E. On peut définir une addition et un produit externe à scalaires dans $\mathbb{K}$ sur $\bigwedge_p^*(E)$. Soient $\phi, \psi \in \bigwedge_p^*(E)$ et $\lambda \in \mathbb{K}$. On pose $\phi + \psi : E \times \ldots \times E \longrightarrow \mathbb{K}$, $(a_1, \ldots, a_p) \mapsto \phi(a_1, \ldots, a_p) + \psi(a_1, \ldots, a_p)$ et $\lambda\phi : E \times \ldots \times E \longrightarrow \mathbb{K}$, $(a_1, \ldots, a_p) \mapsto \lambda\phi(a_1, \ldots, a_p)$. On montre facilement que $(\bigwedge_p^*(E), +, .)$ est un $\mathbb{K}$-espace vectoriel.

Nous allons concentrer notre attention sur l'étude de l'espace vectoriel $\bigwedge_n^*(E)$ des formes n-linéaires alternées sur l'espace vectoriel E de dimension n ($n \in \mathbb{N}^*$). C'est la clef pour introduire la notion de déterminant.

Exercice 6.8 – Soient $n \in \mathbb{N}^*$ et E un $\mathbb{K}$-espace vectoriel de dimension n. A toute base $\mathcal{E} = \{e_1, \ldots, e_n\}$ de E, nous associons l'application

$$\begin{array}{rccc} \det_{\mathcal{E}} & : & E^n & \longrightarrow & \mathbb{K} \\ & & (a_1, \ldots, a_n) & \mapsto & \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1),1} a_{\sigma(2),2} \ldots a_{\sigma(n),n} \end{array}$$

où, pour tout $(a_1, \ldots, a_n) \in E^n$ et tout $j \in \{1, \ldots, n\}$, $a_j = a_{1j}e_1 + \ldots + a_{nj}e_n$ est la décomposition de a_j dans la base $\mathcal{E}$.
1. Montrer que l'application $\det_{\mathcal{E}}$ est une forme n-linéaire alternée sur E. (On pourra utiliser le critère de la proposition 6.6.)
2. Montrer que $\det_{\mathcal{E}}(e_1, \ldots, e_n) = 1$.

Exercice 6.9 –
1) On suppose $n = 2$. Soit $\mathcal{E} = \{e_1, e_2\}$ une base de E. Montrer que, si $a_1 = a_{11}e_1 + a_{21}e_2$ et $a_2 = a_{12}e_1 + a_{22}e_2$ sont deux vecteurs de E, on a $\det_{\mathcal{E}}(a_1, a_2) = \sum_{\sigma \in \mathfrak{S}_2} \varepsilon(\sigma) a_{\sigma(1),1} a_{\sigma(2),2} = a_{11}a_{22} - a_{21}a_{12}$. (On rappelle que $\mathfrak{S}_2 = \{\mathrm{id}_2, (1,2)\}$.)
2) On suppose $n = 3$. Soit $\mathcal{E} = \{e_1, e_2, e_3\}$ une base de E. Montrer que, si $a_1 = a_{11}e_1 + a_{21}e_2 + a_{31}e_3$, $a_2 = a_{12}e_1 + a_{22}e_2 + a_{32}e_3$ et $a_3 = a_{13}e_1 + a_{23}e_2 + a_{33}e_3$ sont trois vecteurs de E, on a $\det_{\mathcal{E}}(a_1, a_2, a_3) = \sum_{\sigma \in \mathfrak{S}_3} \varepsilon(\sigma) a_{\sigma(1),1} a_{\sigma(2),2} a_{\sigma(3),3} = a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{21}a_{12}a_{33} - a_{31}a_{22}a_{13} - a_{11}a_{32}a_{23}$. (On rappelle que $\mathfrak{S}_3 = \{\mathrm{id}_3, (1,2), (1,3), (2,3), (123), (132)\}$.)

Le résultat suivant est fondamental. Il permet, en particulier, d'établir un lien entre $\det_{\mathcal{E}}$ et $\det_{\mathcal{E}'}$ pour deux bases différentes $\mathcal{E}$ et $\mathcal{E}'$.

Théorème 6.10 – *Si E est un $\mathbb{K}$-espace vectoriel de dimension n, alors* $\dim \bigwedge_n^*(E) = 1$.

Remarque 6.11 –
1) On reprend les notations précédentes. Dans la preuve du théorème 6.10 on est amené à montrer que, si ϕ est une forme n-linéaire alternée de l'espace E de dimension n et si $\mathcal{E} = \{e_1, \ldots, e_n\}$ est une base de E, alors $\phi = \phi(e_1, \ldots, e_n) \det_{\mathcal{E}}$. Cela entraîne, en particulier, qu'il existe une unique application ϕ de $\bigwedge_n^*(E)$ qui prend la valeur 1 sur le n-uple $(e_1, \ldots, e_n)$, à savoir $\det_{\mathcal{E}}$.
2) On reprend les notations précédentes et on considère en outre une autre base de E, notée $\mathcal{E}' = \{e'_1, \ldots, e'_n\}$. On peut lui attacher un nouvel élément de $\bigwedge_n^*(E)$, à savoir $\det_{\mathcal{E}'}$. Ce qui précède montre que $\det_{\mathcal{E}'} = \det_{\mathcal{E}'}(e_1, \ldots, e_n) \det_{\mathcal{E}}$.

On peut maintenant définir la notion de déterminant d'une famille de vecteurs dans une base donnée.

Définition 6.12 – *Soit $\mathcal{E} = \{e_1, \ldots, e_n\}$ une base de E et $(a_1, \ldots, a_n)$ un n-uple d'éléments de E, on appelle déterminant de $(a_1, \ldots, a_n)$ dans la base $\mathcal{E}$, le scalaire* $\det_{\mathcal{E}}(a_1, \ldots, a_n)$.

Remarque 6.13 – Il est clair que le déterminant de $(a_1, \ldots, a_n)$ dépend du choix de la base dans laquelle il est calculé. En vertu de 6.11, si $\mathcal{E}' = \{e'_1, \ldots, e'_n\}$ est une autre base de E, le déterminant de $(a_1, \ldots, a_n)$ dans la base $\mathcal{E}'$ est lié au déterminant de $(a_1, \ldots, a_n)$ dans la base $\mathcal{E}$ par $\det_{\mathcal{E}'}(a_1, \ldots, a_n) = \det_{\mathcal{E}'}(e_1, \ldots, e_n) \det_{\mathcal{E}}(a_1, \ldots, a_n)$. C'est-à-dire que $\det_{\mathcal{E}'} = \det_{\mathcal{E}'}(e_1, \ldots, e_n) \det_{\mathcal{E}}$.

Nous définissons maintenant le déterminant d'une matrice.

Définition 6.14 – *Soient $n \in \mathbb{N}^*$ et $A = (a_{ij}) \in M_n(\mathbb{K})$, on appelle déterminant de A le scalaire noté* $\det A$ *et défini par* $\det A = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1),1} a_{\sigma(2),2} \ldots a_{\sigma(n),n}$.

Remarque 6.15 – Soient E un $\mathbb{K}$-espace vectoriel de dimension finie, égale à $n \in \mathbb{N}^*$ et $\mathcal{E} = \{e_1, \ldots, e_n\}$ une base de E. On considère une famille $\{a_1, \ldots, a_n\}$ de vecteurs de E. Par définition, on a

$$\det_{\mathcal{E}}(a_1, \ldots, a_n) = \det \mathrm{Mat}_{\mathcal{E}}(a_1, \ldots, a_n).$$

Pour définir la notion de déterminant d'un endomorphisme il est nécessaire de montrer un résultat préliminaire. Pour ce faire, on utilise les notations suivantes. Soit ϕ une forme n-linéaire alternée de E et u un endomorphisme de E, on note ϕ_u l'application de E^n dans $\mathbb{K}$ définie par $\phi_u(a_1, \ldots, a_n) = \phi(u(a_1), \ldots, u(a_n))$ pour tout n-uple $(a_1, \ldots, a_n)$. Il est très facile de montrer que ϕ_u est encore une forme n-linéaire alternée.

Proposition 6.16 – *Soit u un endomorphisme de E. Il existe un scalaire $k_u \in \mathbb{K}$ tel que, pour toute forme n-linéaire alternée ϕ de E, on ait $\phi_u = k_u \phi$.*

Démonstration : Soit ϕ une forme n-linéaire alternée non nulle de E et u un endomorphisme de E. D'après 6.10, $\bigwedge_n^*(E)$ est de dimension 1. Il existe donc $k_{u,\phi} \in \mathbb{K}$ tel que $\phi_u = k_{u,\phi}\phi$. Pour prouver le théorème, on doit montrer qu'en réalité, $k_{u,\phi}$ ne dépend pas de ϕ. Soit donc ψ une autre forme n-linéaire alternée non nulle. On a de même $\psi_u = k_{u,\psi}\psi$. De plus, il existe $\lambda \in \mathbb{K}$ tel que $\psi = \lambda\phi$ (cf. 6.10). On montre facilement qu'alors $\psi_u = \lambda\phi_u$ Ainsi, $k_{u,\psi}\lambda\phi = k_{u,\psi}\psi = \psi_u = \lambda\phi_u = \lambda k_{u,\phi}\phi$. Il s'ensuit que $k_{u,\psi} = k_{u,\phi}$. On note k_u la valeur commune des $k_{u,\psi}$ et on a donc $\phi_u = k_u\phi$ pour toute forme n-linéaire alternée ϕ non nulle. Comme cette relation reste vraie si $\phi = 0$, la preuve est complète. ∎

D'après la proposition précédente, la définition suivante à un sens.

Définition 6.17 – *Soit u un endomorphisme de E, on appelle déterminant de u le scalaire noté* $\det u \in \mathbb{K}$ *et tel que pour tout $\phi \in \bigwedge_n^*(E)$ on ait $\phi_u = (\det u)\phi$.*

Remarque 6.18 – Soit u un endomorphisme de E.
1) Si $\mathcal{E} = \{e_1, \ldots, e_n\}$ est une base de E, on doit avoir $(\det_{\mathcal{E}})_u = (\det u) \det_{\mathcal{E}}$. En particulier, $(\det_{\mathcal{E}})_u(e_1, \ldots, e_n) = (\det u)\ \det_{\mathcal{E}}(e_1, \ldots, e_n) = \det u$. Donc,

$$\det u = \det_{\mathcal{E}}(u(e_1), \ldots, u(e_n)).$$

2) Soit $\mathcal{E} = \{e_1, \ldots, e_n\}$ une base de E et A la matrice de u relativement à $\mathcal{E}$. En reprennant la définition de $\det A$ et celle de $\det_{\mathcal{E}}$, on montre facilement que $\det u = \det A$.

Nous terminons par quelques propriétés immédiates du déterminant.

Proposition 6.19 – *Soient u et v des endomorphismes de E, on a les propriétés suivantes :*
(i) $\det \mathrm{id}_E = 1$ *;*
(ii) $\det(uv) = \det u \, \det v$ *;*
(iii) $\det u \neq 0$ *ssi u est inversible, et si u est inversible,* $\det u^{-1} = (\det u)^{-1}$.

Démonstration : Le point (i) découle immédiatement de 6.18. Pour obtenir (ii), il suffit de remarquer que, si ϕ est une forme n-linéaire alternée et u et v deux endomorphismes de E, on a $(\phi_v)_u = \phi_{v\circ u}$ et d'appliquer la définition de déterminant d'un endomorphisme. Prouvons le point (iii). On suppose d'abord que u est inversible, alors (i) et (ii) montrent que $\det(u)\det(u^{-1}) = \det(uu^{-1}) = \det \mathrm{id}_E = 1$. Donc, si u est inversible, $\det u \neq 0$ et $\det u^{-1} = (\det u)^{-1}$. Il reste donc à prouver que si $\det u \neq 0$, u est inversible. Montrons la contraposée : si u n'est pas inversible alors $\det u = 0$. C'est facile : considérons une base $\mathcal{E} = \{e_1, \ldots, e_n\}$ de E. Dire que u n'est pas inversible entraîne que la famille $(u(e_1), \ldots, u(e_n))$ est liée. Or, on a vu en 6.5 que ceci conduit à $\det_{\mathcal{E}}(u(e_1), \ldots, u(e_n)) = 0$. Joint au fait que $\det u = \det_{\mathcal{E}}(u(e_1), \ldots, u(e_n)) = 0$ (cf. 6.18), on a $\det u = 0$. ∎

La proposition 6.19 à la conséquence suivante, très importante car elle montre que le déterminant d'une famille de n vecteurs permet de déterminer si cette famille est libre.

Corollaire 6.20 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}^*$ et $\mathcal{E}$ une base de E. Soit $\{a_1, \ldots, a_n\}$ une famille de n vecteurs de E. Alors, $\{a_1, \ldots, a_n\}$ est libre si et seulement si* $\det_{\mathcal{E}}\{a_1, \ldots, a_n\} \neq 0$.

Démonstration : Exercice très instructif. On pourra considérer l'endomorphisme de E défini par : pour $1 \leq i \leq n$, $u(e_i) = a_i$ et appliquer la proposition 6.19. ∎

Proposition 6.21 – *Soient A et B des matrices de $M_n(\mathbb{K})$, on a les propriétés suivantes :*
(i) $\det \mathrm{I}_n = 1$ *;*
(ii) $\det(AB) = \det A \, \det B$ *;*
(iii) $\det A \neq 0$ *ssi A est inversible, et si A est inversible,* $\det A^{-1} = (\det A)^{-1}$ *;*
(iv) si $\lambda \in \mathbb{K}$; alors $\det(\lambda A) = \lambda^n \det A$.

Démonstration : Si on fixe une base de E, A et B peuvent être considérés comme les matrices représentatives de deux endomorphismes u et v de E relativement à cette base. Il reste à combiner le second point de 6.18 et 6.19 pour démontrer les points (i), (ii) et (iii). Le point (iv) se déduit immédiatement de la définition du déterminant d'une matrice. ∎

Les propriétés suivantes sont utiles dans la pratique.

Proposition 6.22 – *Soit $A \in M_n(\mathbb{K})$; alors* $\det A = \det {}^tA$.

Démonstration : Cette propriété se déduit de la définition du déterminant d'une matrice. ∎

Remarque 6.23 – La proposition précédente permet de transférer des colonnes aux lignes les procédés de calcul liés à la n-linéarité du déterminant et au fait qu'il est alterné. Ainsi, si une des lignes est combinaison linéaire des autres, le déterminant de la matrice est nul. De même, on sait que si l'on permute deux colonnes dans une matrice, le déterminant change de signe (cf. 6.6). La même propriété est donc vraie pour les lignes, etc.

On décrit maintenant des méthodes pratiques de calcul des déterminants.

On commence par une définition utile.

Définition 6.24 – *Soit $n \in \mathbb{N}^*$ et $A \in M_n(\mathbb{K})$. Pour $1 \leq p \leq n$, on appelle mineur de format $p \times p$ tout déterminant d'une matrice extraite de A de format $p \times p$.*

La première règle de calcul est dite *règle de calcul par bloc*.

Proposition 6.25 – *Soit $M \in M_n(\mathbb{K})$ une matrice de la forme*

$$M = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix},$$

où $A \in M_p(\mathbb{K})$, $B \in M_q(\mathbb{K})$, $C \in M_{p,q}(\mathbb{K})$ et $p + q = n$. Alors, $\det M = (\det A)(\det B)$.

La seconde règle de calcul est dite *règle de développement suivant une rangée*. Elle nécessite d'introduire un peu de vocabulaire.

Soit $A = (a_{i,j}) \in M_n(\mathbb{K})$. Pour tout couple $(i, j) \in \mathbb{N}_n \times \mathbb{N}_n$, on note $A_{i,j}$ la matrice de $M_{n-1}(\mathbb{K})$ obtenue en ignorant la ligne i et la colonne j dans A. Par ailleurs, on appelle cofacteur du coefficient $a_{i,j}$ de A le scalaire $(-1)^{i+j} \det A_{i,j}$. On a alors la proposition suivante.

Proposition 6.26 – *Avec les notations précédentes :*
(1) $\forall j \in \mathbb{N}_n$, $\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A_{i,j}$ *(développement suivant la j-ème colonne) ;*
(2) $\forall i \in \mathbb{N}_n$, $\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det A_{i,j}$ *(développement suivant la i-ème ligne).*

On termine par un théorème qui permet le calcul des inverses de matrices. Pour ceci, a toute matrice A, on associe sa comatrice $\mathrm{com}A$ dont le terme de i-ème ligne et j-ème colonne est le cofacteur de a_{ij}, c'est-à-dire $(-1)^{i+j} \det A_{i,j}$. On a alors le théorème suivant.

Théorème 6.27 – *Soit $A \in M_n(\mathbb{K})$,* $A\,{}^t(\mathrm{com}A) = {}^t(\mathrm{com}A)A = (\det A) I_n$.

Corollaire 6.28 – *Soit $A \in M_n(\mathbb{K})$. Si A est inversible, alors*

$$A^{-1} = \frac{1}{\det A} ({}^t\mathrm{com}A).$$

Les résultats sur le déterminant d'une matrice décrits ci-dessus permettent de reformuler et préciser certains énoncés de la section 5 portant sur le rang. C'est le cas, en particulier, du théorème 5.35 et de son corollaire 5.36. Il s'ensuit des reformulations de certains résultats portant sur la résolution des systèmes linéaires comme le théorème 5.44.

En outre, on a le résultat suivant, qui donne des formules explicites, dites *formules de Cramer*, pour les solutions des systèmes de Cramer.

Soit (A, b) un système de Cramer à n équations et n inconnues (*i.e.*, $A = (a_{ij}) \in M_n(K)$, $b = (b_i) \in M_{n,1}(\mathbb{K})$ avec A inversible). Pour $1 \leq i \leq n$, notons B_i la matrice obtenue en substituant l'unique colonne de b à la i-ième colonne de A. Alors, si l'on note $(x_1, \ldots, x_n)$ l'unique solution du système (A, b), on a

$$\forall\, 1 \leq i \leq n,\ x_i = \frac{\det B_i}{\det A}.$$

Pour référence ultérieure, on termine ce chapitre par la définition de la notion d'*orientation* pour un $\mathbb{R}$-espace vectoriel de dimension finie.

Soient $n \in \mathbb{N}^*$ et E un $\mathbb{R}$-espace vectoriel de dimension n. Si $\mathcal{E} = \{e_1, \ldots, e_n\}$ et $\mathcal{E}' = \{e'_1, \ldots, e'_n\}$ sont deux bases de E, on a

$$\det_{\mathcal{E}}(e'_1, \ldots, e'_n) = \det P_{\mathcal{E},\mathcal{E}'}.$$

A l'aide de la proposition 6.21, on montre que la relation binaire portant sur l'ensemble de toutes les bases de E et définie, pour deux bases $\mathcal{E}$ et $\mathcal{E}'$, par

$$\mathcal{E}\,\mathcal{R}\,\mathcal{E}' \quad \text{si} \quad \det P_{\mathcal{E},\mathcal{E}'} > 0$$

est une relation d'équivalence. Il est clair que cette relation d'équivalence détermine deux classes d'équivalence. Orienter le $\mathbb{R}$-espace vectoriel E signifie choisir une de ces deux classes. Les bases de la classe choisie sont dites *directes*, celles de l'autre classe sont dites *indirectes*.

7 Réduction des endomorphismes et des matrices carrées.

Dans cette section, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

Définition 7.1 – *Soit E un $\mathbb{K}$-espace vectoriel, F un sous-espace vectoriel de E et u un endomorphisme de E. On dit que F est stable par u si $u(F) \subseteq F$.*

Exercice 7.2 – Soit E un $\mathbb{K}$-espace vectoriel et u et v deux endomorphismes de E. Montrer que si u et v commutent (*i.e.* $u \circ v = v \circ u$), alors $\mathrm{im}u$ et $\ker u$ sont stables par v.

Définition 7.3 – *Soit E un $\mathbb{K}$-espace vectoriel et u un endomorphisme de E.*
1. Soit $P = a_0 + a_1X + \ldots + a_nX^n$ ($n \in \mathbb{N}^*$) un élément de $\mathbb{K}[X]$. On note $P(u)$ l'endomorphisme de E défini par $P(u) = a_0\mathrm{id}_E + a_1u + \ldots + a_nu^n$.
2. On appelle polynôme de l'endomorphisme u tout élément v de $\mathcal{L}(E)$ tel qu'il existe $P \in \mathbb{K}[X]$ vérifiant $v = P(u)$.

Exercice 7.4 – Soit E un $\mathbb{K}$-espace vectoriel et u un endomorphisme de E.
1. Vérifier, à la main, que l'ensemble I_u des éléments P de $\mathbb{K}[X]$ tels que $P(u) = 0$ est un idéal de $\mathbb{K}[X]$ et que le sous-ensemble des éléments de $\mathcal{L}(E)$ qui sont des polynômes de l'endomorphisme u est une sous-algèbre commutative de $\mathcal{L}(E)$ (c'est, en fait, la sous-algèbre de $\mathcal{L}(E)$ engendrée par u).
2. Montrer que l'application

$$\begin{array}{rccc} \mathrm{ev}_u & : & \mathbb{K}[X] & \longrightarrow & \mathcal{L}(E) \\ & & P & \mapsto & P(u) \end{array}$$

est un morphisme de $\mathbb{K}$-algèbres. En déduire que l'ensemble I_u des éléments P de $\mathbb{K}[X]$ tels que $P(u) = 0$ est un idéal de $\mathbb{K}[X]$ et que le sous-ensemble des éléments de $\mathcal{L}(E)$ qui sont des polynômes de l'endomorphisme u est une sous-algèbre commutative de $\mathcal{L}(E)$.
3. Montrer que si E est de dimension finie, I_u n'est pas nul. (On pourra remarquer qu'alors $\mathcal{L}(E)$ est un $\mathbb{K}$-espace vectoriel de dimension finie.)

Remarque 7.5 – Soit E un $\mathbb{K}$-espace vectoriel et u un endomorphisme de E. Comme $\mathbb{K}[X]$ est un anneau principal, l'idéal I_u est principal. Il s'ensuit qu'il existe un unique polynôme unitaire μ_u de $\mathbb{K}[X]$, appelé polynôme minimal de u, tel que I_u soit l'idéal de $\mathbb{K}[X]$ engendré par μ_u. Bien qu'il soit passé sous silence dans la suite de ce résumé, le polynôme minimal est important pour prouver certains résultats apparaissant dans la suite et concernant les sous-espaces caractéristiques.

Proposition 7.6 – *Soient E un $\mathbb{K}$-espace vectoriel, u un endomorphisme de E et P, Q deux éléments de $\mathbb{K}[X]$ premiers entre eux. Alors, on a* $\ker(PQ)(u) = \ker P(u) \oplus \ker Q(u)$.

Démonstration : Exercice très instructif. On pourra considérer une identité de Bézout entre P et Q. ∎

Définition 7.7 – *Soit E un $\mathbb{K}$-espace vectoriel et u un endomorphisme de E.*
1. Un élément $\lambda \in \mathbb{K}$ est une valeur propre de E si $\ker(u - \lambda \mathrm{id}_E)$ *n'est pas réduit à $\{0\}$.*
2. Si $\lambda \in \mathbb{K}$ est une valeur propre de u, on appelle sous-espace propre de valeur propre λ le sous-espace vectoriel $\ker(u - \lambda \mathrm{id}_E)$.
3. Si $\lambda \in \mathbb{K}$ est une valeur propre de E, on appelle vecteur propre de u de valeur propre λ tout élément non nul de $\ker(u - \lambda \mathrm{id}_E)$.

Proposition 7.8 – *Soient E un $\mathbb{K}$-espace vectoriel et u un endomorphisme de E. Si $\lambda_1, \ldots, \lambda_p$ ($p \in \mathbb{N}^*$) sont p valeurs propres de u deux-à-deux distinctes, alors la somme des sous-espaces propres associés à ces vecteurs propres est directe.*

Démonstration : Exercice facile. ∎

On passe maintenant à la reduction des endomorphismes.

Dans toute la suite de cette section, on se limitera au cas de la dimension finie.

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et u un endomorphisme de E. On peut considérer l'application

$$\begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \mapsto & \det(u - x\mathrm{id}_E) \end{array}.$$

Il n'est pas difficile de vérifier que cette application est polynomiale de degré $\dim E$. (On peut calculer $\det(u - x\mathrm{id}_E)$ comme le déterminant d'une matrice après avoir choisi une base arbitraire.) Le polynôme associé à cette fonction polynomiale est noté P_u.

Définition 7.9 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et u un endomrphisme de E. Dans les notations ci-dessus, P_u est appelé le polynôme caractéristique de u.*

Lemme 7.10 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et u un endomorphisme de E. Soit $\lambda \in \mathbb{K}$. Les assertions suivantes sont équivalentes :*
(i) λ est valeur propre de u ;
(ii) λ est racine de P_u.

Démonstration : Exercice facile et très instructif. ∎

Ainsi, si E est un $\mathbb{K}$-espace vectoriel de dimension finie, u un endomorphisme de E admettant p valeurs propres distinctes ($p \in \mathbb{N}^*$) et si $\lambda_1, \ldots, \lambda_p$ désignent ces valeurs propres, il existe des

entiers strictement positifs $m_1, \ldots, m_p$ (à savoir les ordres de multiplicité respectives des racines $\lambda_1, \ldots, \lambda_p$ de P_u) tels que l'on ait :

$$P_u = \prod_{1 \leq i \leq p} (X - \lambda_i)^{m_i} Q,$$

où Q est un élément de $\mathbb{K}[X]$ n'admettant pas de racines dans $\mathbb{K}$.

On commence par aborder le problème de la trigonalisation des endomorphismes.

Définition 7.11 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. On dit que u est trigonalisable si il existe une base de E relativement à laquelle la matrice représentative de u est triangulaire supérieure.*

Théorème 7.12 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et u un endomorphisme de E. Alors, u est trigonalisable si et seulement si le polynôme caractéristique de u est scindé sur $\mathbb{K}$.*

Démonstration : Elle sera traitée en T.D. ∎

On passe maintenant au problème de la diagonalisation des endomorphismes.

Définition 7.13 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie, u un endomorphisme de E et λ une valeur propre de u. On appelle ordre de multiplicité de la valeur propre λ de u l'ordre de multiplicité de λ comme racine de P_u.*

Proposition 7.14 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie, u un endomorphisme de E et λ une valeur propre de u de multiplicité m_λ. On a :*

$$1 \leq \dim \ker(u - \lambda \mathrm{id}_E) \leq m_\lambda.$$

Démonstration : Exercice très instructif. On pourra considérer une base de $\ker(u - \lambda \mathrm{id}_E)$, la compléter en une base de E, et calculer P_u à l'aide la matrice de u relativement à cette base. ∎

Le théorème suivant est très important.

Théorème 7.15 (Cayley-Hamilton) – *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et u un endomorphisme de E. Alors, $P_u(u) = 0$.*

Définition 7.16 – *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. On dit que u est diagonalisable si il existe une base de E relativement à laquelle la matrice représentative de u est diagonale.*

Lemme 7.17 – Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. Les assertions suivantes sont équivalentes :
(i) u est diagonalisable ;
(ii) il existe une base de E constituée de vecteurs propres de u ;
(iii) E est somme (directe) des sous-espaces propres de u.

Démonstration : Facile et très important. ∎

Exercice 7.18 – Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. Si u est diagonalisable, le polynôme caractéristique de u est scindé.

Théorème 7.19 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. Alors, u est diagonalisable si et seulement si son polynôme caractéristique est scindé et toute valeur propre λ a pour multiplicité la dimension de* $\ker(u - \lambda \mathrm{id}_E)$.

Démonstration : Appliquer le lemme 7.17. ∎

Corollaire 7.20 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. Si le polynôme caractéristique de u est scindé et n'a que des racines simples, alors u est diagonalisable.*

Démonstration : Conséquence immédiate du théorème 7.19. ∎

Théorème 7.21 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. Alors, u est diagonalisable si et seulement si il existe un polynôme $P \in \mathbb{K}[X]$, scindé, n'ayant que des racines simples et tel que $P(u) = 0$.*

Démonstration : Voici les idées principales de la démonstration ; on laisse les détails en exercice.
1. Supposons u diagonalisable et soient $\lambda_1, \ldots, \lambda_p$ ($p \in \mathbb{N}^*$) ses valeurs propres deux-à-deux distinctes. Posons $P = (X - \lambda_1) \ldots (X - \lambda_p)$. On vérifie facilement que $P(u) = 0$. (Par exemple, on peut montrer que $P(u)$ annule tous les éléments d'une base de E constituée de vecteurs propres de u.)
2. On suppose qu'il existe $\lambda_1, \ldots, \lambda_p \in \mathbb{K}$ ($p \in \mathbb{N}^*$) deux-à-deux distinctes tels que, si $P = (X - \lambda_1) \ldots (X - \lambda_p)$, on ait $P(u) = 0$. En appliquant la proposition 7.6, on obtient que $E = \ker(u - \lambda_1 \mathrm{id}_E) \oplus \ldots \oplus \ker(u - \lambda_p \mathrm{id}_E)$. ∎

Lorsqu'on a affaire à un endomorphisme qui n'est pas diagonalisable, on peut tout de même le réduire, si toutefois son polynôme caractéristique est scindé, de façon très satisfaisante. Par exemple, on peut le trigonaliser (cf. théorème 7.12). Mais, en fait, on peut obtenir une réduction bien meilleure (cf. théorème 7.25). C'est ce que l'on va voir maintenant.

Pour cela, la notion pertinente est celle de sous-espace caractéristique.

Définition 7.22 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et u un endomorphisme de E. Si $\lambda \in \mathbb{K}$ est valeur propre de u de multiplicité $m \in \mathbb{N}^*$, le sous-espace caractéristique de u associé à la valeur propre λ est* $\ker(u - \lambda \mathrm{id}_E)^m$.

Exercice 7.23 – Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et u un endomorphisme de E.
1. Les sous-espaces caractéristiques de u sont stables par u.
2. Les sous-espaces caractéristiques de u sont en somme directe. (On pourra utiliser la proposition 7.6.)

Dans toute la suite de cette section, on va donc s'intéresser au cas d'un endomorphisme u de l'espace vectoriel E de dimension $n \in \mathbb{N}^*$, et l'on suppose que P_u est scindé. On fixe alors les notations suivantes : $\lambda_1, \ldots, \lambda_p$ ($p \in \mathbb{N}^*$) désignent les p valeurs propres (deux-à-deux distinctes) de u, dont les multiplicités sont notées $m_1, \ldots, m_p$. Ainsi, on a :

$$P_u = (-1)^n \prod_{1 \leq i \leq p} (X - \lambda_i)^{m_i}.$$

De plus, pour $1 \leq i \leq p$, on note N_i le sous-espace caractéristique de u associé à la valeur propre λ_i.

On a alors le théorème suivante, qui donne une première réduction très utile de u.

Théorème 7.24 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et u un endomorphisme de E. On suppose que le polynôme caractéristique de u est scindé. On a alors :*
1. $E = N_1 \oplus \ldots \oplus N_p$;
2. pour $1 \leq i \leq p$, $\dim N_i = m_i$;
3. pour toute base $\mathcal{B}$ adaptée à la décomposition de E du point 1, la matrice représentative de u dans $\mathcal{B}$ est diagonale par bloc, c'est-à-dire de la forme

$$\begin{pmatrix} B_1 & 0 & \ldots & 0 \\ 0 & B_2 & & 0 \\ \vdots & & \ddots & 0 \\ 0 & \ldots & 0 & B_p \end{pmatrix}$$

où, pour $1 \leq i \leq p$, $B_i \in M_{m_i}(\mathbb{K})$.

Démonstration : Le point 1 est une conséquence facile de la proposition 7.6. Pour le point 2, la preuve est plus délicate. On pourra utiliser le fait que toute valeur propre d'un endomorphisme est racine de son polynôme minimale, en déduire que, pour $1 \leq i \leq p$, la restriction de u à N_i admet λ_i pour seule valeur propre, puis calculer P_u dans une base adaptée à la décomposition de E en somme de sous-espaces caractéristiques. Le point 3 est se déduit facilement de l'exercice 7.23. ∎

Théorème 7.25 – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et u un endomorphisme de E. On suppose que le polynôme caractéristique de u est scindé. On reprend les notations du théorème 7.24. On peut choisir $\mathcal{B}$ de sorte que, pour $1 \leq i \leq p$, la matrice B_i soit triangulaire supérieure et ait tous ses termes diagonaux égaux à λ_i.*

Démonstration : Se déduit des théorèmes 7.24 et 7.12. ∎

Théorème 7.26 (Décomposition de Dunford) – *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et u un endomorphisme de E. On suppose que le polynôme caractéristique de u est scindé. Il existe un unique couple (d, n) d'endomorphismes de E tel que :*
1. $u = d + n$;
2. d est diagonalisable, u est nilpotent ;
3. d et n commutent.

Démonstration : Se déduit, avec un peu de travail (pour l'unicité), du théorème 7.25. ∎

On termine cette section en abordant brièvement la réduction (diagonalisation, trigonalisation, ...) des matrices carrées.

Définition 7.27 – *Soient $n \in \mathbb{N}^*$ et $A \in M_n(\mathbb{K})$.*
1. On dit que A est diagonalisable si il existe une matrice $P \in M_n(\mathbb{K})$, inversible et telle que $P^{-1}AP$ soit une matrice diagonale.
2. On dit que A est trigonalisable si il existe une matrice $P \in M_n(\mathbb{K})$, inversible et telle que $P^{-1}AP$ soit une matrice triangulaire supérieure.

Soient $n \in \mathbb{N}^*$ et $A \in M_n(\mathbb{K})$. On peut considérer l'application

$$\begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \mapsto & \det(A - xI_n) \end{array}.$$

Il n'est pas difficile de vérifier que cette application est polynomiale de degré n. Le polynôme associé à cette fonction polynomiale est noté P_A.

Définition 7.28 – *Soient $n \in \mathbb{N}^*$ et $A \in M_n(\mathbb{K})$. Dans les notations ci-dessus, P_A est appelé le polynôme caractéristique de A.*

Le lien entre la réduction des matrices et celle des endomorphismes est fait dans l'exercice suivant.

Exercice 7.29 – Soient $n \in \mathbb{N}^*$ et $A \in M_n(\mathbb{K})$.
1. On considère une base $\mathcal{B}$ de $\mathbb{K}^n$, arbitrairement choisie, et on note u l'endomorphisme de $\mathbb{K}^n$ dont la matrice dans la base $\mathcal{B}$ est A. Montrer que A est diagonalisable (resp. trigonalisable) si et seulement si u est diagonalisable (resp. trigonalisable). (Dans la pratique, on choisit le plus souvent la base canonique de $\mathbb{K}^n$.)
2. On considère deux bases $\mathcal{B}$ et $\mathcal{C}$ de $\mathbb{K}^n$. Soit u (resp. v) l'endomorphisme de $\mathbb{K}^n$ dont la matrice dans le base $\mathcal{B}$ (resp. $\mathcal{C}$) est A. Montrer que les valeurs propres de u et v sont les mêmes. On peut ainsi définir les valeurs propres de A comme étant les valeurs propres de l'endomorphisme dont A est la matrice représentative pour un choix de base abitraire.

8 *Exercices.*

§A - Espaces vectoriels.

Exercice 8.1 – Pour tout réel $r \in \mathbb{R}$, on considère la fonction $\varepsilon_r : \mathbb{R} \longrightarrow \mathbb{R}$ définie, pour $x \in \mathbb{R}$, par $\varepsilon_r(x) = e^{rx}$.
1. Soient $n \in \mathbb{N} \setminus \{0\}$ et $\{a_i\}_{1 \leq i \leq n}$ une famille d'éléments de $\mathbb{R}$ deux-à-deux distincts. Montrer que la famille $\{\varepsilon_{a_i}\}_{1 \leq i \leq n}$ est une famille libre du $\mathbb{R}$-espace vectoriel des applications de $\mathbb{R}$ dans $\mathbb{R}$.
Indication. On pourra raisonner par récurrence sur n et utiliser une limite en $+\infty$.
2. Soit E un sous-ensemble de $\mathbb{R}$. Montrer que la famille $\{\varepsilon_r\}_{r \in E}$ est une famille libre du $\mathbb{R}$-espace vectoriel des applications de $\mathbb{R}$ dans $\mathbb{R}$.

Exercice 8.2 – Soit E un $\mathbb{K}$-espace vectoriel et $f, g \in \mathcal{L}(E)$.
1. Démontrer que $\operatorname{Ker}(g \circ f) = f^{-1}(\operatorname{Ker} g \cap \operatorname{Im} f)$.
2. On suppose que $f \circ g = g \circ f$. Montrer que $f(\operatorname{Ker} g) \subseteq \operatorname{Ker} g$ et $f(\operatorname{Im} g) \subseteq \operatorname{Im} g$.

Exercice 8.3 – On considère le $\mathbb{R}$-espace vectoriel $\mathbb{R}[X]$ des polynômes à coefficients réels et l'application $f : \mathbb{R}[X] \longrightarrow \mathbb{R}[X]$, $P \mapsto (X+1)P - P(0)$.
1. Démontrer que f est linéaire. Calculer $f(P)(0)$ et $f(P)(-1)$.
2. Déterminer $\operatorname{Ker} f$ et $\operatorname{Im} f$.
3. On note $f^1 = f$ et, pour $n \in \mathbb{N}^*$, on pose $f^{n+1} = f \circ f^n$. Déterminer $\operatorname{Im} f^k$ pour tout entier $k \geq 2$.
4. Soit $g : \mathbb{R}[X] \longrightarrow \mathbb{R}$, $P \mapsto P(-1)$. Déterminer $\operatorname{Ker}(g \circ f)$ et $\operatorname{Im}(g \circ f)$.

Exercice 8.4 – Soit $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$ le $\mathbb{R}$-espace vectoriel des applications de $\mathbb{R}$ dans $\mathbb{R}$. On note F le sous-ensemble de E des applications constantes, G l'ensemble des applications dans E qui s'annulent sur $\mathbb{R}^+$ et H l'ensemble des applications dans E qui s'annulent sur $\mathbb{R}^-$. Montrer que F, G, H sont des sous-espace vectoriels de E et que $E = F \oplus G \oplus H$.

Exercice 8.5 – Soient E, F des $\mathbb{K}$-espaces vectoriels et $f : E \longrightarrow F$ une application linéaire. On considère un sous-espace vectoriel E' de E tel que E' et $\ker f$ soient supplémentaires. On considère en outre l'application linéaire $g : E' \longrightarrow \mathrm{im} f$ induite par f par restrictions des ensembles de départ et d'arrivée. Montrer que g est un isomorphisme.

Exercice 8.6 – Projections.
1. Soient E un $\mathbb{K}$-espace vectoriel, E_1 et E_2 des sous-espaces vectoriels de E supplémentaires. On appelle projection sur E_1 parallèlement à E_2 l'application $p : E \longrightarrow E$ définie ainsi : pour tout $x \in E$, si $x_1 \in E_1$, $x_2 \in E_2$ et $x = x_1 + x_2$, alors $p(x) = x_1$. Montrer que p est une application linéaire, que $\ker p = E_2$, que $\mathrm{im} p = E_1$ et que $p \circ p = p$.
2. Soit $f : E \longrightarrow E$ une application linéaire. Montrer que si $f \circ f = f$, alors il existe des sous-espaces vectoriels E_1 et E_2 de E, supplémentaires dans E et tels que f soit la projection sur E_1 parallèlement à E_2.

Exercice 8.7 – Symétries.
1. Soient E un $\mathbb{K}$-espace vectoriel, E_1 et E_2 des sous-espaces vectoriels de E supplémentaires. On appelle symétrie par rapport à E_1 parallèlement à E_2 l'application $s : E \longrightarrow E$ définie ainsi : pour tout $x \in E$, si $x_1 \in E_1$, $x_2 \in E_2$ et $x = x_1 + x_2$, alors $s(x) = x_1 - x_2$. Montrer que s est une application linéaire bijective et que $s \circ s = \mathrm{id}_E$.
2. Soit $f : E \longrightarrow E$ une application linéaire. Montrer que si $f \circ f = \mathrm{id}_E$, alors il existe des sous-espaces vectoriels E_1 et E_2 de E, supplémentaires dans E et tels que f soit la symétrie par rapport à E_1 parallèlement à E_2.

Exercice 8.8 – Soit E un $\mathbb{R}$-espace vectoriel non nul. On note A le sous-ensemble de $\mathcal{L}(E)$ des applications f telles que $f^2 - 7f + 12\mathrm{id}_E = 0$. Montrer que A est non vide. Dans la suite, on note f un élément de A.
1. Vérifier que $p = f - 3\mathrm{id}_E$ et $q = 4\mathrm{id}_E - f$ sont des projections de E.
2. Calculer $p \circ q$, $q \circ p$, $p + q$. En déduire que $E = \ker(f - 3\mathrm{id}_E) \oplus \ker(f - 4\mathrm{id}_E)$.
3. Pour $n \in \mathbb{N}$, déterminer f^n en fonction de p et q.

Exercice 8.9 – Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f : E \longrightarrow F$ une application linéaire.
1. Montrer que les assertions suivantes sont équivalentes :
(i) f est injective ;
(ii) l'image par f de toute famille libre de E est une famille libre de E ;
(iii) il existe une base de E dont l'image par f est une famille libre de E.
2. Énoncer et démontrer des caractérisations semblables de la surjectivité et de la bijectivité.

§B - Espaces vectoriels de dimension finie.

Exercice 8.10 –
1. Soit $m \in \mathbb{R}$. Déterminer le sous-espace vectoriel de $\mathbb{R}^3$ engendré par les vecteurs $(2, 1, 3)$, $(1, m, 1)$ et $(-1, 1, -m)$. Ces vecteurs sont-ils linéairement indépendants ?
2. Déterminer le sous-espace vectoriel de $\mathbb{R}^3$ engendré par les vecteurs $(3, 2, 1)$, $(4, 1, 1)$ et $(1, 5, 1)$. Ces vecteurs sont-ils linéairement indépendants ?
3. Soit $m \in \mathbb{R}$. Déterminer le sous-espace vectoriel de $\mathbb{R}^3$ engendré par les vecteurs $(m, 1, 1)$, $(1, m, 1)$ et $(1, 1, m)$. Ces vecteurs sont-ils linéairement indépendants ?

Exercice 8.11 – Soit $n \in \mathbb{N}$. On note $\mathbb{R}_n[X]$ le $\mathbb{R}$-espace vectoriel des polynômes à coefficients réels dont le degré est inférieur ou égal à n. Pour $0 \leq k \leq n$, on considère un polynôme P_k de degré k.
1. Montrer que la famille $\{P_k\}_{0\leq k\leq n}$ est libre.
2. Déterminer le sous-espace vectoriel de $\mathbb{R}_n[X]$ engendré par la famille $\{P_k\}_{0\leq k\leq n}$.

Exercice 8.12 – Hyperplans : l'approche naïve.
Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$ et $n \in \mathbb{N}^*$.
1. On considère n éléments $a_1, \ldots, a_n$ de $\mathbb{K}$, qui ne sont pas tous nuls. Montrer que l'ensemble $H = \{(x_1, \ldots, x_n) \in \mathbb{K}^n \,|\, a_1x_1 + \ldots + a_nx_n = 0\}$ est un hyperplan de $\mathbb{K}^n$.
2. Soit H un hyperplan de $\mathbb{K}^n$. Montrer qu'il existe n éléments $a_1, \ldots, a_n$ de $\mathbb{K}$, qui ne sont pas tous nuls, tels que $H = \{(x_1, \ldots, x_n) \in \mathbb{K}^n \,|\, a_1x_1 + \ldots + a_nx_n = 0\}$.
3. Soient $a_1, \ldots, a_n$ n éléments de $\mathbb{K}$ qui ne sont pas tous nuls et $b_1, \ldots, b_n$ n éléments de $\mathbb{K}$ qui ne sont pas tous nuls. Montrer que, si $\{(x_1, \ldots, x_n) \in \mathbb{K}^n \,|\, a_1x_1 + \ldots + a_nx_n = 0\} = \{(x_1, \ldots, x_n) \in \mathbb{K}^n \,|\, b_1x_1 + \ldots + b_nx_n = 0\}$, alors il existe $\lambda \in \mathbb{K}^*$ tel que, pour tout $i \in \{1, \ldots, n\}$, $b_i = \lambda a_i$.

Exercice 8.13 – Soit $n \in \mathbb{N}$. On considère le $\mathbb{R}$-espace vectoriel $\mathbb{R}_n[X]$ des polynômes à coefficients réels de degré au plus n et l'application $\Delta : \mathbb{R}_n[X] \longrightarrow \mathbb{R}_n[X]$, $P \mapsto P(X+1) - P(X)$.
1. Montrer que Δ est un endomorphisme de $\mathbb{R}_n[X]$. Calculer le noyau et l'image de Δ.
2. On suppose $n \geq 2$. Résoudre les équations $\Delta(P) = 1$, $\Delta(P) = X$ et $\Delta(P) = X^2$ en l'inconnue $P \in \mathbb{R}_n[X]$. En déduire, pour $m \in \mathbb{N}$, des expressions simples de $\sum_{k=0}^{m} k$ et $\sum_{k=0}^{m} k^2$.

Exercice 8.14 – Soit $n \in \mathbb{N}$. On considère le $\mathbb{R}$-espace vectoriel $\mathbb{R}_n[X]$ des polynômes à coefficients réels de degré au plus n et l'application $f : \mathbb{R}_n[X] \longrightarrow \mathbb{R}_n[X]$, $P \mapsto P'' + P$.
1. Etudier la linéarité de f, son injectivité, sa surjectivité.
2. Que peut-on en déduire sur les solutions polynomiales de l'équation différentielle $y'' + y = Q$, où $Q \in \mathbb{R}[X]$ est donnée ?

Exercice 8.15 –
1. Soit k un réel. On considère l'application $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ telle que, pour $(x, y, z) \in \mathbb{R}^3$, $f((x, y, z)) = (x + 2y + kz, 2x + ky + 8z)$. Vérifier que f est une application linéaire et déterminer son noyau et son image.
2. On considère l'application $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^4$ telle que, pour $(x, y, z) \in \mathbb{R}^3$, $f((x, y, z)) = (x + 2y - 3z, x + 3y - z, 2x + 5y - 5z, x + 4y - z)$. Vérifier que f est une application linéaire et déterminer son noyau et son image.

Exercice 8.16 – Soit $\sum_{1\leq j\leq n} a_{ij}x_j = 0$ $(1 \leq i \leq p)$ un système de p équations linéaires homogènes à n inconnues et à coefficients dans $\mathbb{K}$. Démontrer que si $n > p$ il admet une solution non nulle. Que peut-on dire si $p \geq n$?

Exercice 8.17 – Soit E un $\mathbb{K}$-espace vectoriel et $f \in \mathcal{L}(E)$. On pose $f^2 = f \circ f$.
1. Comparer $\operatorname{Ker} f$ et $\operatorname{Ker} f^2$ d'une part et $\operatorname{Im} f$ et $\operatorname{Im} f^2$ d'autre part.
2. On suppose que E est de dimension finie.
2.1. Démontrer que les trois assertions suivantes sont équivalentes : (1) $E = \operatorname{Ker} f \oplus \operatorname{Im} f$; (2) $\operatorname{Im} f^2 = \operatorname{Im} f$; (3) $\operatorname{Ker} f^2 = \operatorname{Ker} f$.
2.2. Les propriétés (1) à (3) ci-dessus sont-elles satisfaites si f est un projecteur ? si f est un automorphisme ? pour tout $f \in \mathcal{L}(E)$?
3. Dans cette question, $\mathbb{K} = \mathbb{R}$, $E = \mathbb{R}[X]$ et $f : \mathbb{R}[X] \longrightarrow \mathbb{R}[X]$, $P \mapsto P'$, est la dérivation. Parmi les propriétés (1) à (3), lesquelles sont satisfaites ?
4. Les propriétés (1) à (3) sont-elles équivalentes si E n'est pas de dimension finie.

Exercice 8.18 – Soient E et F deux $\mathbb{K}$-espaces vectoriels tels que $\dim_{\mathbb{K}} E < +\infty$ et V un sous-espace vectoriel de E. Montrer que toute application linéaire $f : V \longrightarrow F$ se prolonge en une application linéaire $g : E \longrightarrow F$.

Exercice 8.19 – Soit $n \in \mathbb{N}$. On considère un polynôme non nul A de $\mathbb{C}[X]$, de degré au plus égal à n. On définit deux applications $q, r : \mathbb{C}_n[X] \longrightarrow \mathbb{C}_n[X]$ de la façon suivante : pour tout $P \in \mathbb{C}_n[X]$, $q(P)$ est le quotient et $r(P)$ le reste dans la division euclidienne de P par A. Montrer que q et r sont des applications linéaires et calculer leur noyau et leur image.

Exercice 8.20 – Dans le $\mathbb{R}$-espace vectoriel $\mathbb{R}^3$, on considère la droite vectoriel $D = \text{Vect}\{(-1, 1, 2)\}$ et l'hyperplan $H = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \,|\, x_1 + 2x_2 - x_3 = 0\}$.
1. Montrer que $\mathbb{R}^3 = D \oplus P$.
2. Déterminer l'expression de la projection sur P parallèlement à D.

Exercice 8.21 – On note $\mathbb{R}^{\mathbb{N}}$ le $\mathbb{R}$-espace vectoriel des suites réelles et l'on pose $E = \{(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}} \,|\, \forall n \in \mathbb{N}, 2u_{n+3} + u_{n+2} - 5u_{n+1} + 2u_n = 0\}$.
1. Montrer que E est un sous-espace vectoriel de $\mathbb{R}^{\mathbb{N}}$.
2. Soit $\varphi : E \to \mathbb{R}^3$ l'application qui à une suite $(u_n)_{n\in\mathbb{N}}$ associe le triplet (u_0, u_1, u_2). Montrer que φ est un isomorphisme d'espaces vectoriels. En déduire la dimension de E.
3. Déterminer toutes les suites géométriques appartenant à E. En déduire une base de E.
4. Déterminer l'élément $(u_n)_{n\in\mathbb{N}}$ de E vérifiant $u_0 = 0$ et $u_1 = u_2 = 1$.
5. Soit $F = \{(u_n)_{n\in\mathbb{N}} \in E \mid u_0 = 0\}$. Vérifier que F est un sous-espace vectoriel de E et en donner une base.

Exercice 8.22 – Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}^*$. On considère un endomorphisme u de E qui commute avec tout élément de $\mathcal{L}(E)$ (*i.e.*, pour tout $v \in \mathcal{L}(E)$, $u \circ v = v \circ u$).
1. Soit x un élément de E non nul. En complétant x en une base de E et en choisissant un endomorphisme judicieux de E, montrer qu'il existe $\lambda_x \in \mathbb{K}$ tel que $u(x) = \lambda_x x$.
2. En déduire, à l'aide de la linéarité de u, que u est une homothétie.

Exercice 8.23 –
1. Soit $n \in \mathbb{N}^*$. Montrer que tout $\mathbb{K}$-espace vectoriel de dimension égale à n est isomorphe à $\mathbb{K}^n$.
Indication. On pourra considérer une base de l'espace vectoriel en question.
2. Montrer que deux espaces vectoriels de dimension finie sont isomorphes si et seulement si ils ont même dimension.

Exercice 8.24 – Soient E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle et H un sous-espace vectoriel de E. Montrer que les assertions suivantes sont équivalentes :
(i) H est un hyperplan de E ;
(ii) pour tout $v \in E \setminus H$, $E = H \oplus \mathbb{K}.v$;
(iii) il existe $v \in E \setminus \{0\}$ tel que $E = H \oplus \mathbb{K}.v$.

Exercice 8.25 – Soit E un $\mathbb{K}$-espace vectoriel de dimension n et $\{\phi_1, \ldots, \phi_n\}$ une base de E^*. Montrer qu'il existe une base de E et une seule dont $\{\phi_1, \ldots, \phi_n\}$ soit la duale.

Exercice 8.26 – On pose $E = \mathbb{R}^3$; les formes linéaires ϕ_1, ϕ_2 et ϕ_3 définies par $\phi_1((x, y, z)) = 2x - y + 3z$, $\phi_2((x, y, z)) = 3x - 5y + z$ et $\phi_3((x, y, z)) = 4x - 7y + z$ forment-elles une base de E^* ?

Exercice 8.27 – On pose $E = \mathbb{R}_2[X]$ et on considère trois formes linéaires sur E, ϕ_0, ϕ_1 et ϕ_2, définies par : $\forall P \in E$, $\phi_0(P) = P(0)$, $\phi_1(P) = P(1)$ et $\phi_2(P) = \int_0^1 P(t)dt$. La famille $\{\phi_1, \phi_2, \phi_3\}$ est-elle une base de E^* ?

Exercice 8.28 – On pose $E = \mathbb{R}^3$ et on considère les formes linéaires ϕ_1, ϕ_2 et ϕ_3 définies par $\phi_1((x, y, z)) = 3x + y + 2z$, $\phi_2((x, y, z)) = 2x + y + 2z$ et $\phi_3((x, y, z)) = 6x + 2y + 5z$. Montrer que $\{\phi_1, \phi_2, \phi_3\}$ est une base de E^* et déterminer la base de E dont elle est la duale.

Exercice 8.29 – On pose $E = \mathbb{R}^3$ et on considère deux réels λ et μ. On définit trois formes linéaires sur E, ϕ_1, ϕ_2 et ϕ_3, par $\phi_1((x, y, z)) = x + \lambda y + \lambda^2 z$, $\phi_2((x, y, z)) = x + \mu^2 y + \mu z$ et $\phi_3((x, y, z)) = x + y + z$. Pour quels choix de λ et μ $\{\phi_1, \phi_2, \phi_3\}$ est-elle une base de E^* ?

Exercice 8.30 – Soit $E = \mathbb{R}_4[X]$. On définit les formes linéaires $\phi_0, \phi_1, \phi_2, \phi_3, \phi_4$ de E^* par : $\forall P \in E$, $\phi_0(P) = P(0)$, $\phi_1(P) = P(1)$, $\phi_2(P) = P'(1)$, $\phi_3(P) = P(-1)$, $\phi_4(P) = P'(-1)$. Montrer que $\{\phi_0, \phi_1, \phi_2, \phi_3, \phi_4\}$ est une base de E^* et déterminer la base de E dont elle est la duale.

Exercice 8.31 – Soit $E = \mathbb{R}^4$ et $\mathcal{B} = \{e_1, e_2, e_3, e_4\}$ la base canonique de E. On considère les vecteurs $v_1 = (2, -1, 4, 0)$ et $v_2 = (-1, 0, 3, 4)$ de E et on pose $V = \text{Vect}\{v_1, v_2\}$.
1. Montrer que $\mathcal{C} = \{e_1, e_2, v_1, v_2\}$ est une base de E.
2. On note $\mathcal{C}^* = \{e_1^*, e_2^*, v_1^*, v_2^*\}$ la duale de $\mathcal{C}$. Montrer qu'un élément x de E est dans V si et seulement si $e_1^*(x) = e_2^*(x) = 0$.
3. Exprimer e_1^* et e_2^* comme combinaison linéaire des éléments de $\mathcal{B}^*$ et en déduire une description de V par des équations.

Exercice 8.32 – On pose $E = \mathbb{R}^4$ et on note $\mathcal{C} = \{e_1, e_2, e_3, e_4\}$ sa base canonique. Soit F le sous-espace de E engendré par les vecteurs $3e_1 - e_2 + e_4$ et $e_1 + e_3$. Déterminer les équations caractérisant F relativement à la base $\mathcal{C}$.

Exercice 8.33 – On pose $E = \mathbb{R}^4$ et on note $\mathcal{C} = \{e_1, e_2, e_3, e_4\}$ sa base canonique. Soit F le sous-espace de E engendré par le vecteur $e_1 + e_2 + e_3 + e_4$. Déterminer les équations caractérisant F relativement à la base $\mathcal{C}$.

Exercice 8.34 – Soit $E = \mathbb{R}_3[X]$. On considère $u \in \mathcal{L}(E)$ définie par : $\forall P \in E$, $u(P)(X) = P'(X + 1) + P'(X - 1) - P'(X)$. Soit enfin $f \in E^*$ définie par : $\forall P \in E$, $f(P) = \int_0^1 P(t)dt$.
a) Déterminer $\phi = {}^t u(f)$, image de f par la transposée de u.
b) On définit les éléments $e_1^*, e_2^*, e_3^*, e_4^*$ de E^* par : $\forall P \in E$, $e_1^*(P) = P(0)$, $e_2^*(P) = P(1)$, $e_3^*(P) = P'(0)$, $e_4^*(P) = P'(1)$. Montrer que $\{e_1^*, e_2^*, e_3^*, e_4^*\}$ forme une base de E^* et trouver la base dont elle et la duale.
c) Calculer les composantes de ϕ dans $\{e_1^*, e_2^*, e_3^*, e_4^*\}$.

Exercice 8.35 – Soit $E = \mathbb{R}^4$.
1) Déterminer l'orthogonal du sous-espace de E engendré par les vecteurs $(1, 0, 1, 0)$ et $(0, 1, 0, 1)$.
2) Déterminer l'orthogonal du sous-espace de E intersection des hyperplans d'équations $x_1 - x_2 + 2x_3 + x_4 = 0$ et $x_1 + 2x_2 - x_3 + x_4 = 0$.

Exercice 8.36 – Soient $n \in \mathbb{N}^*$ et $E = \mathbb{K}_n[X]$ ($\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$). Déterminer la base duale de la base canonique de E.

Exercice 8.37 – Soient $n \in \mathbb{N}^*$ et $E = \mathbb{K}_n[X]$ ($\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$). Soit par ailleurs $a \in \mathbb{K}$. Pour $k \in \{0, \dots, n\}$, on définit $\phi_k \in E^*$ par $\forall P \in E$, $\phi_k(P) = P^{(k)}(a)$. Montrer que $\{\phi_0, \dots, \phi_n\}$ est une base de E^* et déterminer la base de E dont elle est la duale.

Exercice 8.38 – Soit E un espace vectoriel de dimension finie. Montrer que si u est un endomorphisme de E, alors un scalaire α est valeur propre de u ssi α est valeur propre de la transposée de u.

Exercice 8.39 – On pose $E = \mathbb{K}_n[X]$. On considère l'endomorphisme D de dérivation de E : $\forall P \in E$, $D(P) = P'$. Déterminer la transposée de D en donnant l'image par cette application d'une base de E^*.
Même question en substituant à D l'endomorphisme T défini par : $\forall P \in E, T(P)(X) = P(X+1)$.

Exercice 8.40 – **Polynômes d'interpolation de Lagrange.**
On pose $E = \mathbb{K}_n[X]$. Si $a \in \mathbb{K}$, on définit $\phi_a \in E^*$ en posant : $\forall P \in E$, $\phi_a(P) = P(a)$.
1) On considère $n+1$ éléments $a_0, a_1, \dots, a_n$ dans $\mathbb{K}$. Montrer que les $n+1$ formes linéaires $\phi_{a_0}, \dots, \phi_{a_n}$ sont linéairement indépendantes ssi les a_i sont deux-à-deux distincts.
2) On considère $n+1$ éléments $a_0, a_1, \dots, a_n$ dans $\mathbb{K}$, deux-à-deux distincts. Déterminer la base $\{L_0, \dots, L_n\}$ dont $\{\phi_{a_0}, \dots, \phi_{a_n}\}$ est la duale.
3) On considère, à présent, deux familles de $n+1$ scalaires : $\{a_0, a_1, \dots, a_n\}$ et $\{b_0, b_1, \dots, b_n\}$ et on suppose que les éléments de $\{a_0, a_1, \dots, a_n\}$ sont deux-à-deux distincts. Montrer qu'il existe un polynôme P de E et un seul tel que $P(a_i) = b_i$, pour $0 \leq i \leq n$.

Exercice 8.41 – Soit E un $\mathbb{K}$-espace vectoriel de dimension finie.
1. Soit S une partie de E. Montrer que $(S^\perp)^\perp = \mathrm{Vect}(S)$.
1. Soit T une partie de E^*. Montrer que $(T^\perp)^\perp = \mathrm{Vect}(T)$.

Exercice 8.42 – Soit E un $\mathbb{K}$-espace vectoriel, $p \in \mathbb{N}^*$ et $L, \ell_1, \dots, \ell_p$ des formes linéaires sur E. Montrer que les assertions suivantes sont équivalentes :
(i) $\cap_{i=1}^p \ker \ell_i \subseteq \ker L$;
(ii) $L \in \mathrm{Vect}\{\ell_1, \dots, \ell_p\}$.

Exercice 8.43 – Posons $E = \mathbb{R}[X]$. Pour $n \in \mathbb{N}$, on note f_n la forme linéaire sur E qui à un polynôme P de E associe son coefficient d'indice n.
1. Montrer que $\{f_n\}_{n\in\mathbb{N}}$ est une famille libre de E^*.
2. A quelle condition sur a a-t-on la forme linéaire $\mathrm{ev}_a : E \longrightarrow \mathbb{R}$, $P \mapsto P(a)$ est-elle dans $\mathrm{Vect}\{f_n\}_{n\in\mathbb{N}}$?
3. La famille $\{f_n\}_{n\in\mathbb{N}}$ est elle génératrice de E^*.

Exercice 8.44 – **Crochet de dualité et bidual.**
Soit E un $\mathbb{K}$-espace vectoriel.
1. On appelle crochet de dualité l'application

$$\begin{array}{rccc} \langle -,- \rangle & : & E \times E^* & \longrightarrow & \mathbb{K} \\ & & (x, \phi) & \mapsto & \phi(x) \end{array} .$$

Montrer que l'application $\langle -,- \rangle$ est bilinéaire.
2. On note E^{**} le bidual de E, c'est-à-dire le dual du dual de E. Montrer que l'application

$$\begin{array}{rccc} J & : & E & \longrightarrow & E^{**} \\ & & x & \mapsto & \langle x, - \rangle \end{array}$$

est un isomorphisme de $\mathbb{K}$-espaces vectoriels où, pour $x \in E$, $\langle x, - \rangle : E^* \longrightarrow \mathbb{K}$, $\phi \mapsto \langle x, \phi \rangle$.
Indication. Pour montrer que J est injective, on pourra montrer que, si x est un élément non nul, alors $J(x) \neq 0$. Pour ce faire, on pourra compléter $\{x\}$ en une base de E et construire une forme linéaire qui ne s'annule pas sur x.
3. En déduire le résultat suivant : si $\{\phi_1, \ldots, \phi_n\}$ une base de E^*. Il existe une base $\{x_1, \ldots, x_n\}$ de E dont $\{\phi_1, \ldots, \phi_n\}$ est la base duale.

§C - Matrices.

Exercice 8.45 – Déterminer le noyau et l'image de l'endomorphisme f de $\mathbb{R}^3$ dont la matrice relativement à la base canonique de $\mathbb{R}^3$ est $A = \begin{pmatrix} 1 & 1 & -1 \\ -3 & -3 & 3 \\ -2 & -2 & 2 \end{pmatrix}$. En déduire qu'il existe une base de $\mathbb{R}^3$ relativement à laquelle la matrice représentative de f est $B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

Exercice 8.46 – Déterminer le noyau et l'image de l'application linéaire f de $\mathbb{R}^4$ dans $\mathbb{R}^5$ dont la matrice relativement aux bases canonique de $\mathbb{R}^4$ et $\mathbb{R}^5$ est $A = \begin{pmatrix} 1 & -2 & -1 & 3 \\ 5 & 14 & 3 & -1 \\ 2 & 23 & 7 & -1 \\ 0 & 3 & 1 & -2 \\ -1 & 5 & 2 & 0 \end{pmatrix}$.

Exercice 8.47 – On considère les matrices $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ à coefficients réels. Calculer B^n pour $n \in \mathbb{N}^*$. En déduire A^n pour $n \in \mathbb{N}^*$. Démontrer que A est inversible et calculer son inverse.

Exercice 8.48 – On note $\{e_1, e_2, e_3\}$ la base canonique de $\mathbb{R}^3$. On considère les endomorphismes f et g de $\mathbb{R}^3$ définis de la façon suivante. Pour $(x, y, z) \in \mathbb{R}^3$, $f((x, y, z)) = (2x - 3y + 7z, x - y - z, 3x - y)$ et $g(e_1) = e_1 + e_2 + e_3$, $g(e_2) = 5e_1 + e_2 - 3e_3$, $g(e_3) = e_1 - e_3$. Déterminer le noyau et l'image de $g \circ f$.

Exercice 8.49 – Calculer le rang des matrices suivantes à coefficients dans $\mathbb{C}$ (où α et m sont des paramètres complexes) :

$$\begin{pmatrix} 2 & 1 & 1 \\ 5 & 5 & 4 \\ 1 & 8 & 5 \\ 2 & -2 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 2 \\ 2 & 3 & 5 & 1 \\ 1 & 3 & 4 & 5 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 & 1 \\ 2 & 2 & -1 & 3 \\ m & 3 & -2 & 0 \\ -1 & 0 & -4 & 3 \end{pmatrix}, \quad \begin{pmatrix} -1 & \alpha & 0 & \ldots & \ldots & 0 \\ 0 & -1 & \alpha & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ 0 & & & \ddots & -1 & \alpha \\ \alpha & 0 & \ldots & \ldots & 0 & -1 \end{pmatrix}.$$

Exercice 8.50 – Soit S le sous-espace vectoriel de $\mathbb{R}^4$ engendré par les vecteurs colonnes de la

matrice

$$\begin{pmatrix} 1 & 2 & 0 & 1 \\ 2 & 3 & 1 & 0 \\ -1 & 3 & 3 & 1 \\ -2 & -1 & 1 & 0 \end{pmatrix}.$$

1. Quelle est la dimension de S ?
2. Combien d'équations faut-il pour caractériser S ?
3. Donner une famille d'équations dont S soit l'ensemble des solutions.

Exercice 8.51 – La matrice $\begin{pmatrix} 3 & -4 & 1 \\ 2 & -1 & 5 \\ 1 & -1 & 1 \end{pmatrix}$ est-elle inversible ? Si elle l'est, calculer son inverse.

Exercice 8.52 – Soient $m, n \in \mathbb{N}^*$. Dans $M_{m,n}(\mathbb{K})$, on note $\sim$ la relation de similitude (c-à-d celle définie, pour $A, B \in M_{m,n}(\mathbb{K})$, par $A \sim B$ si A et B sont semblables). Les affirmations suivantes sont-elles exactes ? (On demande de justifier la réponse.)
1. $A \sim B$ implique ${}^tA \sim {}^tB$;
2. $A \sim B$ implique $\lambda A \sim \lambda B$, pour $\lambda \in \mathbb{K}$;
3. $A \sim I_n$ implique que A est inversible.
4. $A \sim B$ et $A, B \in GL_n(\mathbb{K})$ implique que $A^{-1} \sim B^{-1}$.
5. $A \sim B$ et $C \sim D$ implique que $A + C \sim B + D$.
5. $A \sim B$ et $C \sim D$ implique que $AC \sim BD$.

§D - Déterminants.

Exercice 8.53 – Donner un moyen simple de calculer le déterminant d'une matrice triangulaire et d'une matrice diagonale.

Exercice 8.54 – Calculer $\det \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$.

Exercice 8.55 – Calculer A^{-1}, où $A = \begin{pmatrix} 2 & 3 & -1 \\ 0 & -1 & -1 \\ 2 & 1 & 2 \end{pmatrix}$.

Exercice 8.56 – Calculer $\det \begin{pmatrix} a^2 & (a+1)^2 & (a+2)^2 \\ b^2 & (b+1)^2 & (b+2)^2 \\ c^2 & (c+1)^2 & (c+2)^2 \end{pmatrix}$, $(a, b, c) \in \mathbb{K}$.

Exercice 8.57 – Déterminer les réels a tels que $\det \begin{pmatrix} 2a+2 & 3 & a \\ 4a-1 & a+1 & 2a-1 \\ 5a-4 & a+1 & 3a-4 \end{pmatrix} = 0$.

Exercice 8.58 – Calculer $\det \begin{pmatrix} 1-x & 1 & 1 & 1 \\ 1 & 1-x & -1 & -1 \\ 1 & -1 & 1-x & -1 \\ 1 & -1 & -1 & 1-x \end{pmatrix}$.

Exercice 8.59 – On considère n éléments de $\mathbb{K}$, $a_1, \ldots, a_n$. Calculer le déterminant de la matrice (dite de Vandermonde) :

$$V(a_1, \ldots, a_n) = \begin{pmatrix} 1 & a_1 & a_1^2 & \ldots & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & \ldots & a_2^{n-1} \\ \vdots & & & & & \vdots \\ 1 & a_n & a_n^2 & \ldots & \ldots & a_n^{n-1} \end{pmatrix}.$$

Exercice 8.60 – Calculer

$$\det = \begin{pmatrix} a_1+b_1 & b_1 & b_1 & \ldots & b_1 & b_1 \\ b_2 & a_2+b_2 & b_2 & \ldots & b_2 & b_2 \\ \vdots & & & & & \vdots \\ b_n & b_n & b_n & \ldots & b_n & a_n+b_n \end{pmatrix}.$$

Exercice 8.61 – Calculer

$$\det \begin{pmatrix} a_n & a_{n-1} & \ldots & \ldots & \ldots & \ldots & a_0 \\ -1 & x & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & -1 & x & 0 & \ldots & \ldots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \ldots & \ldots & 0 & -1 & x & 0 \\ 0 & \ldots & \ldots & \ldots & 0 & -1 & x \end{pmatrix}.$$

Exercice 8.62 – Soient $a, b, c \in \mathbb{C}$. On pose

$$D_n = \det \begin{pmatrix} a & b & 0 & \ldots & \ldots & \ldots & 0 \\ c & a & b & 0 & \ldots & \ldots & 0 \\ 0 & c & a & b & 0 & \ldots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \ldots & 0 & c & a & b & 0 \\ 0 & \ldots & \ldots & 0 & c & a & b \\ 0 & \ldots & \ldots & \ldots & 0 & c & a \end{pmatrix}.$$

1. Montrer que la suite $(D_n)_{n\in\mathbb{N}^*}$ est une suite récurrente linéaire de degré 2.
2. Calculer D_n, $n \in \mathbb{N}^*$, pour $a = 1$, $b = 1$ et $c = -2$.

Exercice 8.63 – On appelle matrice circulante une matrice de $M_n(\mathbb{C})$ qui a la forme suivante :

$$C(a_1, \ldots, a_n) = \begin{pmatrix} a_1 & a_2 & \ldots & \ldots & \ldots & \ldots & a_n \\ a_n & a_1 & a_2 & \ldots & \ldots & \ldots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \ldots & \ldots & \ldots & a_{n-2} \\ \vdots & & & & & & \vdots \\ a_2 & a_3 & \ldots & \ldots & \ldots & a_n & a_1 \end{pmatrix}$$

où $a_1, \ldots, a_n$ sont des complexes. On désigne par $z_1, \ldots, z_n$ les racines n-èmes de l'unité dans $\mathbb{C}$ et on pose $P(X) = a_1 + a_2X + a_3X^2 + \ldots + a_nX^{n-1}$. Enfin, on note U la transposée de la matrice de Vandermonde $V(z_1, \ldots, z_n)$.
1) Calculer $C(a_1, \ldots, a_n)U$.
2) En déduire l'expression de $\det C(a_1, \ldots, a_n)$ à l'aide de $P(z_1), \ldots, P(z_n)$.

Exercice 8.64 – **Déterminant par blocs.**
1. On veut montrer que si A et B désignent des matrices carrées et C une matrice, on a :

$$\det \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = (\det A) \cdot (\det B).$$

1.1. Montrer le résultat si A n'est pas inversible.
1.2. On suppose A inversible. Montrer que :

$$\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} I & A^{-1}C \\ 0 & B \end{pmatrix}.$$

En déduire la formule.
1.3. Trouver quatre matrices carrées A, B, C, D de même taille telles que :

$$\det \begin{pmatrix} A & D \\ B & C \end{pmatrix} \neq (\det A) \cdot (\det C) - (\det B) \cdot (\det D).$$

2. Soient A, B, C, D quatre matrices carrées de même taille. On leur associe la matrice carrée :

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

On suppose que $CD = DC$.
2.1. On suppose que D est inversible. Montrer que $\det M = \det(AD - BC)$. Pour cela, on calculera $M \times \begin{pmatrix} D & 0 \\ -C & D^{-1} \end{pmatrix}$.
2.2. On suppose D non inversible. On considère l'application $f : \mathbb{R} \to \mathbb{R}$ définie par :

$$f(x) = \det \begin{pmatrix} A & B \\ C & D - xI \end{pmatrix}.$$

En utilisant la continuité de cette application, montrer qu'on a encore : $\det M = \det(AD - BC)$.
2.3. Soit $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$, montrer que $AB \neq BA$.
Soit $M = \begin{pmatrix} A & B \\ B & A \end{pmatrix}$, calculer $\det M$ et $\det(A^2 - B^2)$.

§E - Réduction des endomorphismes et des matrices carrées.

Exercice 8.65 – Le but de cet exercice est de montrer le résultat suivant. Soient E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $u \in \mathcal{L}(E)$; les assertions suivantes sont équivalentes :
(i) u est trigonalisable,
(ii) le polynôme caractéristique de u est scindé.
En fait, la démonstration de ce résultat fournit aussi un moyen pratique de trigonalisation.
1. Montrer que (i) implique (ii).
2. Soit u un endomorphisme de E dont le polynôme caractéristique, P_u, est scindé.
2.1. Montrer que u admet une valeur propre.
2.2. Soit λ une valeur propre de u. Montrer que $\mathrm{im}(u - \lambda \mathrm{id})$ est une sous-espace vectoriel de E de dimension au plus égale à $n - 1$.
2.3. Montrer qu'il existe un hyperplan H de E tel que $\mathrm{im}(u - \lambda \mathrm{id}) \subseteq H$. Montrer que pour tout tel hyperplan, on a $u(H) \subseteq H$.

2.4. Montrer qu'il existe une base de E relativement à laquelle la matrice de u est de la forme suivante :

$$\begin{pmatrix} a_{11} & \dots & \dots & a_{1,n-1} & a_{1n} \\ \vdots & & & \vdots & \vdots \\ \vdots & & & \vdots & \vdots \\ a_{n-1,1} & \dots & \dots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & \dots & \dots & 0 & \lambda \end{pmatrix}.$$

2.5. On note v la restriction de u à H. Montrer que le polynôme caractéristique de v est scindé.
2.6. Conclure.

Exercice 8.66 – des cas suivants, on note u l'endomorphisme de $\mathbb{R}^3$ dont la matrice dans la base canonique est A. Étudier la diagonalisabilité et la trigonalisabilité de u et, le cas échéant, diagonaliser ou trigonaliser u.

1. $A = \begin{pmatrix} -8/5 & 0 & -2/5 \\ 0 & -2 & 0 \\ -8/5 & 0 & -2/5 \end{pmatrix}$.
2. $A = \begin{pmatrix} -2 & 8 & 6 \\ -4 & 10 & 6 \\ 4 & -8 & -4 \end{pmatrix}$.
3. $A = \begin{pmatrix} 8 & -1 & -5 \\ -2 & 3 & 1 \\ 4 & -1 & -1 \end{pmatrix}$.
4. $A = \begin{pmatrix} 2 & -2 & 3 \\ 10 & -4 & 5 \\ 5 & -4 & 6 \end{pmatrix}$.
5. $A = \begin{pmatrix} -7 & 2 & -3 \\ -4 & 0 & -2 \\ 5 & -2 & 1 \end{pmatrix}$.
6. $A = \begin{pmatrix} -4 & -2 & -4 \\ -2 & 0 & 0 \\ 2 & -2 & -2 \end{pmatrix}$.

Exercice 8.67 – Soit f l'endomorphisme de $\mathbb{R}^4$ dont la matrice représentative dans la base canonique de $\mathbb{R}^4$ est

$$\begin{pmatrix} 6/5 & -2/5 & 1/5 & 1/5 \\ -2/5 & 9/5 & -2/5 & 3/5 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Montrer que f est diagonalisable et diagonaliser f.

Exercice 8.68 – On pose $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$. Soit u l'endomorphisme de $\mathbb{K}^3$ dont la matrice dans la base canonique est $A = \begin{pmatrix} 0 & -2 & 0 \\ 1 & 0 & -1 \\ 0 & 2 & 0 \end{pmatrix}$. Suivant que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$, u est-il diagonalisable, trigonalisable ? Si oui, le diagonaliser, le trigonaliser. Calculer A^n pour $n \in \mathbb{N}$.

Exercice 8.69 – Soient a, b deux complexes ; on pose $A = \begin{pmatrix} a & b & b \\ b & a & b \\ b & b & a \end{pmatrix}$.
1. Déterminer les valeurs du couple (a, b) pour lequel A est non inversible.
2. Calculer A^n pour $n \in \mathbb{N}$ lorsque A n'est pas inversible. Calculer A^n pour $n \in \mathbb{Z}$ lorsque A est inversible.

Exercice 8.70 – Trouver une matrice carrée M de $M_4(\mathbb{C})$ telle que $M^2 = A$ où A est la matrice de $M_4(\mathbb{C})$ dont tous les cefficients sont égaux à 1 sauf ceux de la diagonale qui sont nuls. (On peut commencer par diagonaliser A.)

Exercice 8.71 – Donner une condition nécessaire et suffisante pour que la matrice $A = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & d & e \\ 0 & 0 & 2 & f \\ 0 & 0 & 0 & 2 \end{pmatrix}$
de $M_4(\mathbb{R})$ soit diagonalisable.

Exercice 8.72 – Soit E un espace vectoriel de dimension finie et u un endomorphisme diagonalisable de E. Montrer que $E = \ker u \oplus \mathrm{im} u$.

Exercice 8.73 – Soit E un espace vectoriel de dimension finie. Montrer que tout projecteur et que toute symétrie est diagonalisable.

Exercice 8.74 – On pose $E = \mathbb{R}_n[X]$ et ϕ l'endomorphisme de E défini par $\phi(P) = (X^2 - 1)P'' + (2X + 1)P'$ pour $P \in E$.
1) Ecrire la matrice de ϕ dans la base canonique de E.
2) Déterminer les valeurs propres de ϕ.
3) Montrer que les vecteurs propres associés à la valeur propre $i(i + 1)$ sont des polynômes de degré i.

Exercice 8.75 – Pour chacune des matrices A suivantes, calculer A^n pour $n \in \mathbb{N}^*$
- en utilisant la réduction de A,
- en utilisant le théorème de Cayley-Hamilton ;

$A = \begin{pmatrix} 8 & -1 & -5 \\ -2 & 3 & 1 \\ 4 & -1 & -1 \end{pmatrix}$, $A = \begin{pmatrix} 0 & a & a^2 \\ a^{-1} & 0 & a \\ a^{-2} & a^{-1} & 0 \end{pmatrix}$ $(a \in \mathbb{R}^*)$, $A = \begin{pmatrix} 3 & -1 & 1 & -1 \\ 1 & 3 & 1 & 1 \\ -1 & 1 & 1 & 1 \\ -1 & 1 & -3 & 5 \end{pmatrix}$.

Partie VII

Géométrie vectorielle euclidienne.

1 Produit scalaire, norme euclidienne.

Dans cette section, on définit et on étudie en détail la structure géométrique d'un espace vectoriel euclidien.

Définition 1.1 – *Soit E un $\mathbb{R}$-espace vectoriel de dimension $n \in \mathbb{N}^*$. On appelle produit scalaire sur E une forme bilinéaire symétrique définie positive, c'est-à-dire une application bilinéaire*

$$\begin{array}{rccc} \phi & : & E \times E & \longrightarrow & \mathbb{R} \\ & & (x,y) & \mapsto & \phi(x,y) \end{array}$$

vérifiant les propriétés suivantes :
(i) pour tout $y \in E$, l'application partielle à gauche $\phi(-,y) : E \longrightarrow \mathbb{R}$, $x \mapsto \phi(x,y)$ et l'application partielle à droite $\phi(y,-) : E \longrightarrow \mathbb{R}$, $x \mapsto \phi(y,x)$ sont des formes linéaires ;
(ii) pour tous $x, y \in E$, $\phi(x,y) = \phi(y,x)$;
(iii) pour tout $x \in E$, $\phi(x,x) = 0$ entraîne $x = 0$;
(iv) pour tout $x \in E$, $\phi(x,x) \geq 0$.

Remarque 1.2 – Dans la pratique, si l'on veut vérifier qu'une application $\phi : E \times E \longrightarrow \mathbb{R}$ est bilinéaire symétrique, on vérifie d'abord la symétrie (point (ii) de la définition 1.1) puis, pour vérifier la bilinéarité (condition (i) de la définition 1.1), il suffit de montrer que les applications partielles à gauche sont linéaires, la linéarité des applications à droite s'en déduisant immédiatement.

Définition 1.3 – On appelle espace vectoriel euclidien un couple (E, ϕ), où E est un $\mathbb{R}$-espace vectoriel de dimension finie et $\phi : E \times E \longrightarrow \mathbb{R}$ un produit scalaire.

Notation 1.4 – *Soit (E, ϕ) un espace vectoriel euclidien. Pour tout $x \in E$, on pose $||x||_\phi = \sqrt{\phi(x,x)}$.*

Proposition 1.5 – *Soit (E, ϕ) un espace vectoriel euclidien.*
1. Pour tout $x \in E$, $||x||_\phi = 0$ si et seulement si $x = 0$.
2. Pour tout $x \in E$ et tout $\lambda \in \mathbb{R}$, $||\lambda x||_\phi = |\lambda|\, ||x||_\phi$.
3. Pour tous $x, y \in E$, on a :
3.1. $2\phi(x,y) = ||x+y||_\phi^2 - ||x||_\phi^2 - ||y||_\phi^2$ (identité de polarisation) ;
3.2. $||x+y||_\phi^2 + ||x-y||_\phi^2 = 2(||x||_\phi^2 + ||y||_\phi^2)$ (identité du parallélogramme) ;
3.3. $|\phi(x,y)| \leq ||x||_\phi ||y||_\phi$ (inégalité de Cauchy-Schwarz) ;
3.4 $||x+y||_\phi \leq ||x||_\phi + ||y||_\phi$ (inégalité triangulaire).

Démonstration : Les points 1 et 2 sont immédiats. Soient à présent $(x,y) \in E \times E$. On a, compte tenu de la bilinéarité et de la symétrie de ϕ,

$$||x+y||_\phi^2 = \phi(x+y, x+y) = \phi(x,x) + \phi(y,y) + 2\phi(x,y) = ||x||||_\phi^2 + ||y||_\phi^2 + 2\phi(x,y),$$

ce qui établit l'identité de polarisation. Il s'ensuit que, pour tout $\lambda \in \mathbb{R}$, on a

$$||x+\lambda y||_\phi^2 = ||x||_\phi^2 + \lambda^2 ||y||_\phi^2 + 2\lambda\phi(x,y).$$

La fonction $\mathbb{R} \longrightarrow \mathbb{R}$, $\lambda \mapsto ||x+\lambda y||_\phi^2$ est donc une fonction polynomiale à valeurs dans $\mathbb{R}^+$. On en déduit qu'elle n'a pas de racines ou une double, c'est-à-dire que son discriminant $4\phi(x,y)^2 - 4||x||_\phi^2 ||y||^2$ est négatif ou nul. L'inégalité de Cauchy-Schwarz s'en déduit immédiatement. A

forciori, on a $2\phi(x,y) \leq 2||x||_\phi||y||_\phi$, et donc $2\phi(x,y)+||x||_\phi^2+||y||_\phi^2 \leq 2||x||_\phi||y||_\phi+||x||_\phi^2+||y||_\phi^2$, qui s'écrit encore $2\phi(x,y)+||x||_\phi^2+||y||^2 \leq (||x||_\phi+||y||_\phi)^2$. Donc, compte tenu de l'identité de polarisation, on a $||x+y||_\phi^2 \leq (||x||_\phi+||y||_\phi)^2$, qui donne facilement l'inégalité triangulaire.

Enfin, soit $(x,y) \in E \times E$. L'identité de polarisation appliquée au couples (x,y) et $(x,-y)$ de $E \times E$ donne facilement l'identité du parallélogramme. ∎

Corollaire 1.6 – *Soit (E,ϕ) un espace vectoriel euclidien. L'application*

$$\begin{array}{rccc} \|-\|_\phi & : & E & \longrightarrow & \mathbb{R} \\ & & x & \mapsto & \|x\|_\phi \end{array}$$

est une norme de l'espace vectoriel E.

Démonstration : C'est une conséquence immédiate de la Proposition 1.5. ∎

Il est souvent confortable, dans la pratique, d'alléger les notations. Ainsi, dans la suite, si (E,ϕ) est un espace euclidien, on notera souvent, pour $x,y \in E$, $(x|y)$ au lieu de $\phi(x,y)$ et $||x||$ au lieu de $||x||_\phi$. Bien sûr, cette simplification est à proscrire si plusieurs structures euclidiennes sont considérées simultanément sur le même espace.

Exemple 1.7 – **Structure euclidienne standard de $\mathbb{R}^n$, $n \in \mathbb{N}^*$.** Soit $n \in \mathbb{N}^*$. L'application

$$\begin{array}{rcl} \mathbb{R}^n \times \mathbb{R}^n & \longrightarrow & \mathbb{R} \\ ((x_1,\ldots,x_n),(y_1,\ldots,y_n)) & \mapsto & \sum_{i=1}^n x_i y_i \end{array}$$

est un produit scalaire sur $\mathbb{R}^n$. La structure d'espace euclidien ainsi définit sur $\mathbb{R}^n$ sera appelée structure euclidienne standard. La norme associée à cette structure euclidienne est donc

$$\begin{array}{rcl} \mathbb{R}^n & \longrightarrow & \mathbb{R} \\ (x_1,\ldots,x_n) & \mapsto & \sqrt{\sum_{i=1}^n x_i^2} \end{array}$$

Exemple 1.8 – Soit $n \in \mathbb{N}^*$. L'application

$$\begin{array}{rcl} \mathbb{R}_n[X] \times \mathbb{R}_n[X] & \longrightarrow & \mathbb{R} \\ (P,Q) & \mapsto & \displaystyle\int_0^1 P(t)Q(t)dt \end{array}$$

est un produit scalaire sur $\mathbb{R}_n[X]$.

On termine cette section par l'expression matricielle d'un produit scalaire relativement au choix d'une base de l'espace vectoriel ambient.

On peut exprimer un produit scalaire sous forme matricielle relativement à une base donnée. Soit E un espace euclidien dont le produit scalaire est noté $(-|-)$ et soit $\mathcal{E} = \{e_1,\ldots,e_n\}$ une base de E. On appelle matrice de $(-,-)$ relativement à $\mathcal{E}$ la matrice symétrique (c'est-à-dire égale à sa transposée)

$$\mathrm{Mat}_{\mathcal{E}}((-,-)) = ((e_i|e_j))_{1\leq i,j\leq n}.$$

Soient alors $x = x_1e_1+\ldots+x_ne_n$ et $y = y_1e_1+\ldots+y_ne_n$ des vecteurs de E, on a (par bilinéarité) :

$$(x|y) = (x_1e_1+\ldots+x_ne_n|y_1e_1+\ldots+y_ne_n) = \sum_{1\leq i,j\leq n} x_iy_j(e_i|e_j).$$

De sorte que, si $X = \mathrm{Mat}_{\mathcal{E}}(x)$ et $Y = \mathrm{Mat}_{\mathcal{E}}(y)$ sont les matrices colonnes représentatives de x et y relativement à $\mathcal{E}$, et en posant $A = \mathrm{Mat}_{\mathcal{E}}((-|-))$, il vient

$$(x|y) = {}^tXAY.$$

(Notons au passage que, dans l'identité ci-dessus, on commet l'abus de notation qui consiste à confondre un scalaire et la matrice à une ligne et une colonne dont ce scalaire est le seul coefficient.)

Analysons, à présent, l'effet d'un changement de base sur la matrice représentative de $(-|-)$. Soit $\mathcal{F} = \{f_1, \ldots, f_n\}$ une base de E et soit P la matrice de passage de $\mathcal{E}$ à $\mathcal{F}$. Soit enfin A' la matrice représentative de $(-|-)$ relativement à $\mathcal{F}$. Si x et y sont des élément de E dont on note X et Y les matrices respectives relativement à $\mathcal{E}$ et , X' et Y' les matrices respectives relativement à $\mathcal{F}$, alors :

$${}^tX'A'Y' = (x|y) = {}^tXAY = {}^t(PX')A'PY' = {}^tX'{}^tPA'PY'$$

L'égalité ci-dessus étant vrai pour tous $x, y \in E$ et donc pour toutes matrices colonnes X, Y, il s'ensuit que l'on a l'égalité

$$A' = {}^tPAP$$

qui relie les matrices représentatives de $(-|-)$ relativement à $\mathcal{E}$ et $\mathcal{F}$.

2 Orthogonalité.

Définition 2.1 – *Soit E un espace vectoriel euclidien.*
1. Deux éléments $x, y \in E$ sont dits orthogonaux si $(x|y) = 0$.
2. Soit F un sous-espace vectoriel de E. On note $F^\perp$ l'ensemble des vecteurs de E qui sont orthogonaux à tout vecteur de F : $F^\perp = \{y \in E \,|\, \forall x \in F,\, (x|y) = 0\}$.

Proposition 2.2 – ***Théorème de Pythagore.***
Soit E un espace vectoriel euclidien. Deux éléments x, y de E sont orthogonaux si et seulement si $||x + y||^2 = ||x||^2 + ||y||^2$.

Démonstration : C'est une conséquence immédiate de l'identité de polarisation. ∎

Proposition 2.3 – *Soit E un espace vectoriel euclidien.*
1. On a : $E^\perp = \{0\}$.
2. Soit F un sous-espace vectoriel de E.
2.1. On a : $F^\perp$ est un sous-espace vectoriel de E.
2.2. Si $\{f_1, \ldots, f_p\}$ est une base de F, alors un élément x de E est dans $F^\perp$ si et seulement si $(x|f_i) = 0$ pour $1 \leq i \leq p$.

Démonstration : Un élément de $E^\perp$ est en particulier orthogonal à lui-même, ce qui implique qu'il est nul. Ce qui établi le premier point. Le second est une conséquece immédiate de la bilinéarité du produit scalaire. ∎

Définition 2.4 – *Soit E un espace vectoriel euclidien. Soit $\mathcal{E} = \{e_1, \ldots, e_n\}$ une base de E.*
1. On dit que $\mathcal{E}$ est une base orthogonale de E si, pour $1 \leq i \neq j \leq$, e_i et e_j sont orthogonaux.
2. On dit que $\mathcal{E}$ est une base orthognormale de E si c'est une base orthogonale et si, de plus, tous les vecteurs de E sont de norme 1.

Exemple 2.5 – Soit $n \in \mathbb{N}^*$. La base canonique de $\mathbb{R}^n$ est une base orthonormale pour le produit scalaire standard de $\mathbb{R}^n$.

Remarque 2.6 – Soit E un espace vectoriel euclidien de dimension $n \in \mathbb{N}^*$ et $\mathcal{E} = \{e_1, \ldots, e_n\}$ une base orthonormée de E. Alors :
1. La matrice du produit scalaire est la matrice identité I_n.
2. Si la décomposition de x sur $\mathcal{B}$ est $x = x_1e_1 + \ldots + x_ne_n$, alors, pour $1 \leq i \leq n$, $x_i = (x|e_i)$.
Pour x, y dans E, si X et Y sont les matrices colonnes représentatives de x et y respectivement dans la base $\mathcal{B}$, alors

$$(x|y) = {}^tXY.$$

On poursuit par une remarque très utile dans la pratique.

Remarque 2.7 – Soient $\mathcal{E}$ et $\mathcal{F}$ deux bases orthonormales de l'espace vectoriel euclidien E de dimension $n \in \mathbb{N}^*$. Soit P la matrice de passage de $\mathcal{E}$ à $\mathcal{F}$. Soient enfin $x, y \in E$, X, X' les matrices représentatives de x relativement à $\mathcal{E}$ et $\mathcal{F}$ et Y, Y' les matrices représentatives de y relativement à $\mathcal{E}$ et $\mathcal{F}$. On a $X = PX'$ et $Y = PY'$. Il s'ensuit que $(x|y) = {}^tXY = {}^t(PX')(PY) = {}^tX'{}^tPPY'$. Comme on a par ailleurs $(x|y) = {}^tX'Y'$, il vient que ${}^tX'{}^tPPY' = (x|y) = {}^tX'Y'$. On en déduit facilement que

$${}^tPP = I_n.$$

Il n'est pas clair, à priori, que tout espace vectoriel euclidien possède une base orthonormale. En fait c'est le cas, comme le montre le résultat suivant.

Théorème 2.8 – ***Orthogonalisation de Gram-Schmidt.***
Soient E un espace vectoriel euclidien et $\mathcal{E} = \{e_1, \ldots, e_n\}$ une base de E. Il existe une famille $\mathcal{F} = \{f_1, \ldots, f_n\}$ et une seule de vecteurs de E telle que :
1. pour $1 \leq i \neq j \leq n$, $(f_i|f_j) = 0$;
2. pour $1 \leq i \leq n$, $f_i - e_i \in \mathrm{Vect}\{f_j,\ 1 \leq j < i\}$.
En particulier, pour $1 \leq i \leq n$, $\mathrm{Vect}\{e_j,\ 1 \leq j \leq i\} = \mathrm{Vect}\{f_j,\ 1 \leq j \leq i\}$ et $\mathcal{F}$ est une base orthogonale de $\mathcal{E}$.

Démonstration : On laisse au lecteur le soin d'écrire la démonstration de ce résultat, à l'aide d'une récurrence sur la dimension de E. ∎

Le théorème ci-dessus peut en fait se traduire en une méthode pratique, dite *d'orthogonalisation*, d'une base arbitraire de E. On décrit maintenant cette méthode, très utile dans la pratique.

Soit donc E un espace vectoriel euclidien et $\mathcal{E} = \{e_1, \ldots, e_n\}$ une base de E. On cherche une famille orthogonale $\mathcal{F} = \{f_1, \ldots, f_n\}$ de vecteurs de E telle que, pour $1 \leq i < j \leq n$, il existe des scalaires $\alpha_{ij} \in \mathbb{R}$ satisfaisant aux relations :

$$\begin{aligned}
&f_1 = e_1\ ,\\
&f_2 = e_2 + \alpha_{12}f_1\ ,\\
&\vdots\\
&\vdots\\
&f_n = e_n + \alpha_{n-1,n}f_{n-1} + \ldots + \alpha_{1,n}f_1.
\end{aligned}$$

Il reste à construire f_1, f_2, f_3, etc, de proche en proche.
1-ère étape : construction de f_1. Trivial.
2-ème étape : construction de f_2. La condition d'orthogonalité entre f_1 et f_2 est équivalente à

$$\alpha_{12} = -\frac{(f_1|e_2)}{(f_1|f_1)}.$$

Puisque f_1 et e_2 sont connus, on obtient une (et une seule) valeur pour α_{12}. D'où l'on déduit f_2.
etc
(p+1)-ème étape : construction de f_{p+1}, ($p < n$). Supposons obtenus les vecteurs $f_1, \ldots, f_p$. Pour $1 \leq i \leq p$, la condition d'orthogonalité de f_{p+1} avec f_i est équivalente à

$$\alpha_{i,p+1} = -\frac{(f_i|e_{p+1})}{(f_i|f_i)}.$$

Puisque $f_1, \ldots, f_p$ et e_{p+1} sont connus, on obtient une (et une seule) valeur pour $\alpha_{i,p+1}$, $1 \leq i \leq p$. D'où l'on déduit f_{p+1}.

Définition 2.9 – *Soient E un espace vectoriel euclidien, $\mathcal{E} = \{e_1, \ldots, e_n\}$ une base de E et $\mathcal{F} = \{f_1, \ldots, f_n\}$ la base orthogonale de $\mathcal{E}$ construite au théorème 2.8. La base $\mathcal{F}$ est appelée* l'orthogonalisée de $\mathcal{E}$ *et sa normalisation (obtenue en multipliant chaque élément de $\mathcal{F}$ par l'inverse de sa norme) est appelée* l'orthonormalisée de $\mathcal{E}$.

Corollaire 2.10 – *Dans tout espace vectoriel euclidien, il existe une base orthonormale.*

Démonstration : Soit E un espace vectoriel euclidien. Il existe une base de E. Le procédé d'orthogonalisation de Gram-Schmidt permet alors de construire l'orthonormalisée de cette base pour conclure. ∎

Exemple 2.11 – On se place dans l'espace vectoriel $\mathbb{R}^3$ muni de sa structure euclidienne standard. On pose $e_1 = (1, 2, -1)$, $e_2 = (1, 3, 0)$ et $e_3 = (1, -1, 5)$. Il est facile de vérifier que $\mathcal{E} = \{e_1, e_2, e_3\}$ est une base de $\mathbb{R}^3$. L'orthogonalisée de $\mathcal{E}$ est alors l'unique famille orthogonale $\mathcal{F} = \{f_1, f_2, f_3\}$ de vecteurs de $\mathbb{R}^3$ telle qu'il existe des réels $\alpha_{12}, \alpha_{23}, \alpha_{13}$ vérifiant

$$\begin{aligned} f_1 &= e_1 \ , \\ f_2 &= e_2 + \alpha_{12} f_1 \ , \\ f_3 &= e_3 + \alpha_{23} f_2 + \alpha_{13} f_1. \end{aligned}$$

1-ère étape : construction de f_1. On a $f_1 = e_1 = (1, 2, -1)$.
2-ème étape : construction de f_2. On a $0 = (f_1|f_2) = (e_1|e_2) + \alpha_{12}(e_1|e_1)$, ce qui donne $0 = 7 + \alpha_{12}.6$, puis $\alpha_{12} = -7/6$ et donc $f_2 = (-1/6, 2/3, 7/6)$.
3-ème étape : construction de f_3. On a $0 = (f_1|f_3) = (e_1|e_3) + \alpha_{23}(f_1|f_2) + \alpha_{23}(f_1|f_1)$, ce qui donne $0 = -6 + \alpha_{13}.6$, puis $\alpha_{13} = 1$. Avec $0 = (f_2|f_3)$, on trouve de même $\alpha_{13} = -30/11$. Il s'ensuit que $f_3 = (27/11, -9/11, 9/11)$.

L'orthonormalisée de $\mathcal{E}$ s'obtient ensuite en normalisant $\mathcal{F}$. Or, $||f_1|| = \sqrt{6}$, $||f_2|| = \sqrt{11/6}$ et $||f_3|| = 9/\sqrt{11}$. On obtient dont la base orthonormale $\{1/\sqrt{6} f_1, \sqrt{6/11} f_2, \sqrt{11}/9 f_3\}$.

Théorème 2.12 – *(du supplémentaire orthogonal.)*
Soit E un espace vectoriel euclidien et F un sous-espace vectoriel de E. On a

$$E = F \oplus F^{\perp}.$$

En particulier, $\dim E = \dim F + \dim F^{\perp}$.

Démonstration : On note $n, p \in \mathbb{N}$ les dimensions respectives de E et F. Soit $\{e_1, \ldots, e_p\}$ une base de F. On complète $\{e_1, \ldots, e_p\}$ en une base $\{e_1, \ldots, e_n\}$ de E et l'on considère son orthonormalisée $\{f_1, \ldots, f_n\}$. Par definition de l'orthonormalisée, on a $F = \mathrm{Vect}\{f_1, \ldots, f_p\}$.

Soit $x \in E$. Il est clair que $x \in F^\perp$ si et seulement si $(x|f_i) = 0$, pour $1 \leq i \leq p$. Ceci joint au second point de la remarque 2.6 montre que $x \in F^\perp$ si et seulement si $x_i = 0$, pour $1 \leq i \leq p$, c'est-à-dire si et seulement si $x \in \mathrm{Vect}\{e_{p+1}, \ldots, e_n\}$. On a donc montré que $F^\perp = \mathrm{Vect}\{e_{p+1}, \ldots, e_n\}$. Le résultat s'en déduit immédiatement. ∎

3 Adjoint d'un endomorphisme ; endomorphismes symétriques.

Exercice 3.1 – **Isomorphisme canonique d'un espace euclidien avec son dual.**
Soit E un espace vectoriel euclidien dont on note $(-,-)$ le produit scalaire et E^* l'espace dual. Montrer que l'application

$$\begin{array}{rccc} \iota & : & E & \longrightarrow & E^* \\ & & x & \mapsto & (x, -) \end{array}$$

est un isomorphisme d'espaces vectoriels.

Proposition 3.2 – *Soit E un espace vectoriel euclidien. Si u est un endomorphisme de E, il existe un endomorphisme u^* de E et un seul tel que, pour tous $x, y \in E$, $(u(x)|y) = (x|u^*(y))$.*

Démonstration : On admet ce résultat dont la démonstration utilise l'isomorphisme canonique entre un espace vectoriel euclidien et son dual (Exercice 3.1. ∎

Définition 3.3 – *Soit E un espace vectoriel euclidien. Si u est un endomorphisme de E, l'endomorphisme u^* associé à u par la Proposition 3.2 est appelé l'adjoint de u.*

Proposition 3.4 – *Soit E un espace vectoriel euclidien et u un endomorphisme de E. Si $\mathcal{E}$ est une base orthonormée de E, alors* $\mathrm{Mat}_{\mathcal{E}}(u^*) = {}^t\mathrm{Mat}_{\mathcal{E}}(u)$.

Démonstration : On note $n \in \mathbb{N}^*$ la dimension de E et $\mathcal{E} = \{e_1, \ldots, e_n\}$. Posons

$$A = (a_{ij})_{1 \leq i,j \leq n} = \mathrm{Mat}_{\mathcal{E}}(u) \quad \text{et} \quad B = (b_{ij})_{1 \leq i,j \leq n} = \mathrm{Mat}_{\mathcal{E}}(u^*).$$

Soient $1 \leq i, j \leq n$. On a

$$u(e_i) = \sum_{1 \leq k \leq n} a_{ki} e_k \quad \text{et} \quad u^*(e_j) = \sum_{1 \leq k \leq n} b_{kj} e_k.$$

Mais, en utilisant la remarque 2.6, on a

$$a_{ji} = (u(e_i)|e_j) = (e_i|u(e_j)) = b_{ij}.$$

Ceci montre que ${}^t A = B$. ∎

Exemple 3.5 – On se place dans l'espace vectoriel $\mathbb{R}^3$ muni de sa structure euclidienne standard et on note $\mathcal{E} = \{e_1, e_2, e_3\}$ sa base canonique. On considère l'endomorphisme u de $\mathbb{R}^3$ défini par

$$u(e_1) = e_1 + 2e_2 - e_3 \ , \qquad u(e_2) = e_1 + e_3 \ , \qquad u(e_3) = e_2 + 2e_3.$$

D'après la proposition 3.4, on a

$$\mathrm{Mat}_{\mathcal{E}}(u^*) = {}^t\mathrm{Mat}_{\mathcal{E}}(u) = \begin{pmatrix} 1 & 2 & -1 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}.$$

Ainsi, u^* est l'endomorphisme de $\mathbb{R}^3$ défini par

$$u^*(e_1) = e_1 + e_3\ , \qquad u^*(e_2) = 2e_1 + e_3\ , \qquad u^*(e_3) = -e_1 + e_2 + 2e_3.$$

Proposition 3.6 – *Soit E un espace vectoriel euclidien, u, v des endomorphismes de E et $\alpha, \beta \in \mathbb{R}$. On a*
1. $(\alpha u + \beta v)^* = \alpha u^* + \beta v^*$ *;*
2. $(u^*)^* = u$ *;*
3. $(u \circ v)^* = v^* \circ u^*$.

Démonstration : Exercice. On peut utiliser la proposition 3.4. ∎

Définition 3.7 – *Soit E un espace vectoriel euclidien et u un endomorphisme de E. On dit que u est symétrique (ou auto-adjoint) si $u^* = u$.*

Remarque 3.8 – Soit E un espace vectoriel euclidien et u un endomorphisme de E. Il découle immédiatement des définitions que l'endomorphisme u est symétrique si et seulement si, pour tous $x, y \in E$, $(u(x)|y) = (x|u(y))$.

On rappelle qu'un matrice carrée (à coefficients dans un corps quelconque) est dite symétrique si elle est égale à sa transposée.

Proposition 3.9 – *Soit E un espace vectoriel euclidien et u un endomorphisme de E. Les assertions suivantes sont équivalentes :*
(i) u est symétrique ;
(ii) la matrice de u relativement à toute base orthonormée de E est symétrique ;
(iii) il existe une base orthonormée de E relativement à laquelle la matrice de u est symétrique.

Démonstration : La première assertion implique la seconde d'après la proposition 3.4 ; la seconde implique la troisième puisqu'il existe des bases orthonormée (cf. Corollaire 2.10) ; la troisième implique la première d'après la proposition 3.4. ∎

Lemme 3.10 – *Soit E un espace vectoriel euclidien. Si u est un endomorphisme symétrique de E, alors u admet une valeur propre.*

Démonstration : Soit u un endomorphisme symétrique de E. Si $\mathcal{E}$ est une base orthonormée de E et A la matrice de u relativement à A, alors A est symétrique (cf. Proposition 3.9). On peut considérer A comme une matrice à coefficients complexes. Comme toute matrice à coefficients complexes admet une valeur propre, il existe $\lambda \in \mathbb{C}$ et une matrice colonne X non nulle à coefficients dans $\mathbb{C}$ tels que $AX = \lambda X$. On a alors ${}^tXA\overline{X} = {}^tX{}^tA\overline{X} = {}^t(AX)\overline{X} = \lambda({}^tX\overline{X})$ et ${}^tXA\overline{X} = {}^tX\overline{A}\,\overline{X} = {}^tX\overline{AX} = \overline{\lambda}({}^tX\overline{X})$. Comme X est non nul, on a ${}^tX\overline{X} \neq 0$. Ce qui précède montre donc que $\lambda \in \mathbb{R}$. Ainsi, la matrice à coefficients complexes $A - \lambda I_n$ (où $n = \dim E$) n'est pas inversible. Mais, $A - \lambda I_n$ est en fait à coefficients réels. Donc elle n'est pas inversible non plus comme telle : ceci montre que $u - \lambda\mathrm{id}_E$ n'est pas inversible, c'est-à-dire que λ est valeur propre de u.

Théorème 3.11 – *Soit E un espace vectoriel euclidien. Si u est un endomorphisme symétrique de E, alors u est diagonalisable dans une base orthonormée.*

Démonstration : On procède par récurrence sur la dimension de E. Le cas où la dimension de E est 1 est trivial. Supposons donc que n soit un entier tel que tout endomorphisme symétrique d'un espace euclidien de dimension $n \in \mathbb{N}^*$ soit diagonalisable dans une base orthonormée. On considère un espace euclidien E de dimension $n+1$ et un endomorphisme u de E, symétrique. Le lemme 3.10 assure que u admet une valeur propre λ. Soit $x \in E$ tel que $u(x) = \lambda x$. On pose $F = (\mathbb{R}x)^\perp$. On vérifie facilement que le sous-espace vectoriel F de E est stable par u. Soit v la restriction de u à F. Alors, l'espace euclidien F (muni de la restriction du produit scalaire de E) est de dimension n et l'hypothèse de récurrence s'applique : il existe une base orthonormée $\mathcal{E}$ de F constituée de vecteurs propres de v. Il est clair alors que $\mathcal{E}$ complétée par x est une base orthonormée de F constituée de vecteurs propres de u. ∎

Au-delà du résultat d'existence donné par le théorème 3.11 se pose la question de la détermination d'une base orthonormée de vecteurs propres d'un endomorphisme symétrique. En fait, la démonstration du théorème 3.11 légèrement adaptée donne une procédure de détermination d'une telle base de proche en proche. Cependant, il s'avère qu'on peut procéder de façon beaucoup plus efficace, comme l'atteste la remarque suivante.

Lemme 3.12 – *Soit E un espace vectoriel euclidien. Si u est un endomorphisme symétrique de E, et si $\lambda, \mu \in \mathbb{R}$ sont deux valeurs propres distinctes de u, alors les sous-espaces propres E_λ et E_μ respectivement associés sont orthogonaux.*

Démonstration : Soient $x \in E_\lambda$ et $y \in E_\mu$. On a $\lambda(x|y) = (u(x)|y) = (x|u(y)) = \mu(x|y)$. Il s'ensuit que $(x|y) \neq 0$. ∎

Remarque 3.13 – **Pratique de diagonalisation des endomorphismes symétriques.** Soit E un espace vectoriel euclidien et u est un endomorphisme symétrique de E. Le thèorème 3.11 assure alors qu'il existe une base orthonormée de vecteurs propres de u. Le lemme 3.12 permet en fait de mettre au point un moyen simple d'en calculer une. Une fois identifié chaque sous espace propre de u, on peut déterminer dans chacun d'eux une base orthonormée (par exemple en en prenant une quelquonque et en l'orthonormalisant). On peut ensuite considérer la réunion des diverses bases ainsi obtenues. Le théorème 3.11 assure qu'on obtient de cette façon une base et le Lemme 3.12 assure qu'elle est orthonormée.

Théorème 3.14 – *Soit A une matrice symétrique réelle de $M_n(\mathbb{R})$, $n \in \mathbb{N}^*$. Il existe une matrice diagonale D de $M_n(\mathbb{R})$ et une matrice inversible P de $M_n(\mathbb{R})$ vérifiant ${}^tP = P^{-1}$ telles que $D = P^{-1}AP$.*

Démonstration : Les détails sont laissés en exercice. Il s'agit de la version matricielle du théorème 3.11. ∎

4 Endomorphismes orthogonaux.

Définition 4.1 – *Soient E un espace vectoriel euclidien et u un endomorphisme de E.*
1. On dit que u est orthogonal si

$$\forall\, x, y \in E, \qquad (u(x)|u(y)) = (x, y).$$

2. On dit que u est une isométrie si

$$\forall\, x \in E, \qquad ||u(x)|| = ||x||.$$

Remarque 4.2 – Soient E un espace vectoriel euclidien et u un endomorphisme de E.
1. On suppose u orthogonal. Il découle immédiatement de la définition que si $x, y \in E$ sont orthogonaux, alors leurs images $u(x)$ et $u(y)$ le sont aussi.
2. L'endomorphisme u est orthogonal si et seulement si il est une isométrie. En effet, la condition est trivialement nécessaire ; elle est aussi suffisante par la formule de polarisation.

Exercice 4.3 – Soit E un espace vectoriel euclidien et $f : E \longrightarrow E$ une application (quelconque).
1. On dit que f conserve le produit scalaire si, pour tous $x, y \in E$, $(f(x)|f(y)) = (x|y)$. Montre que si f conserve le produit scalaire, alors elle est linéaire.
2. On dit que f conserve la norme si, pour tout $x \in E$, $\|f(x)\| = \|x\|$. Une application qui conserve la norme est-elle nécessairement linéaire ?

Proposition 4.4 – *Soient E un espace vectoriel euclidien et u un endomorphisme de E. L'endomorphisme u est orthogonal si et seulement si il est inversible d'inverse égal à son adjoint u^*.*

Démonstration : Exercice. ∎

Proposition 4.5 – *Soient E un espace vectoriel euclidien et u un endomorphisme de E. Les assertions suivantes sont équivalentes :*
(i) u est orthogonal ;
(ii) l'image par u de toute base orthonormée est une base orthonormée ;
(iii) il existe une base orthonormée dont l'image par u soit une base orthonormée.

Démonstration : (i) $\Longrightarrow$ (ii) D'après la proposition 4.4, u est inversible de sorte que l'image d'une base de E en est encore une. Il suffit d'urtiliser la remarque 4.2 pour voir que si la base de départ est choisie orthogonale, sa transformée par u l'est encore.
(i) $\Longrightarrow$ (ii) C'est trivial puisqu'il existe des bases orthonormées.
(iii) $\Longrightarrow$ (i) Soit $\mathcal{E} = \{e_1, \ldots, e_n\}$ une base orthonormée de E telle que $\{u(e_1), \ldots, u(e_n)\}$ soit une base orthonormée de E. Soient $x, y \in E$, si la décomposition de x (resp. y) sur $\mathcal{E}$ est $x = x_1e_1 + \ldots + x_ne_n$ (resp. $y = y_1e_1 + \ldots + y_ne_n$), en utilisant la remarque 2.6, il vient que

$$(u(x)|u(y)) = \sum_{1\leq i,j\leq n} x_iy_j(u(e_i)|u(e_j)) = \sum_{1\leq i,j\leq n} x_iy_j\delta_{ij} = \sum_{1\leq i,j\leq n} x_iy_j(e_i|e_j) = (x|y).$$

Ceci termine la démonstration. ∎

Définition 4.6 – *Soit $n \in \mathbb{N}$. Une matrice M de $M_n(\mathbb{R})$ est dite orthogonale si ${}^tMM = I_n$.*

Proposition 4.7 – *Soient E un espace vectoriel euclidien et u un endomorphisme de E. Les assertions suivantes sont équivalentes :*
(i) u est orthogonal ;
(ii) pour toute base orthonormée $\mathcal{E}$ de E, $\mathrm{Mat}_{\mathcal{E}}(u)$ est orthogonale ;
(iii) il existe une base orthonormée $\mathcal{E}$ de E telle que $\mathrm{Mat}_{\mathcal{E}}(u)$ soit orthogonale.

Démonstration : Exercice (on pourra s'inspirer de la preuve de la proposition 3.9). ∎

Corollaire 4.8 – *Soient $\mathcal{E}$ une base orthonormée de $E = \{e_1, \ldots, e_n\}$ et $\mathcal{F} = \{f_1, \ldots, f_n\}$ une base quelconque de E. On note P la matrice de passage de $\mathcal{E}$ à $\mathcal{F}$. Alors, $\mathcal{F}$ est une base orthonormée si et seulement si P est orthogonale.*

Démonstration : Si l'on suppose $\mathcal{F}$ orthonormée, la remarque 2.7 s'applique et montre que P est orthogonale. Réciproquement, supposons que P soit orthogonale. En fait, P est la matrice représentative dans $\mathcal{E}$ de l'endomorphisme u tel que, pour $1 \leq i \leq n$, $u(e_i) = f_i$. De l'orthogonalité de P on déduit, par la proposition 4.5, que u est un endomorphisme orthogonal. Les propositions 4.4 et 3.4 montrent alors que P est orthogonale. ∎

Le prochain résultat porte sur la théorie spectrale des endomorphismes orthogonaux.

Théorème 4.9 – *Soit E un espace vectoriel euclidien et u un endomorphisme orthogonal de E.*
1. Si F est un sous-espace vectoriel de E stable par u, alors $F^\perp$ est stable par u.
2. Si $\lambda \in \mathbb{R}$ est valeur propre de u, alors $\lambda \in \{-1, 1\}$.
3. Si -1 et 1 sont valeurs propres de u, alors les espaces propres correspondants sont orthogonaux.
4. Le déterminant de u est 1 ou -1.

Démonstration : 1. Comme u est orthogonal, c'est un automorphisme. Il s'ensuit que sa restriction à F est aussi un automorphisme. Soit alors $x \in F$, $y \in F^\perp$. Il existe $z \in F$ tel que $x = u(z)$. On a donc

$$(x|u(y)) = (u(z)|u(y)) = (z|y) = 0,$$

ce qui montre que $u(F^\perp) \subseteq F^\perp$.
2. Si λ est valeur propre de u, il existe un vecteur x non nul de $x \in E$ tel que $u(x) = \lambda x$. On a alors $||x|| = ||u(x)|| = |\lambda|.||x||$, de sorte que $|\lambda| = 1$ puisque x est non nul.
3. Soient x, y des vecteurs propres de u de valeurs propres respectives 1 et -1. On a $(x|y) = (u(x)|u(y)) = -(x|y)$. Il s'ensuit que $(x|y) = 0$.
4. Soit $\mathcal{E}$ une base orthonormée de E et A la matrice de u relativement à $\mathcal{E}$. La proposition 4.7 montre que A est orthogonale, ce dont on déduit immédiatement que son déterminant vaut 1 ou -1. ∎.

On termine par quelques mots sur le groupe orthogonal.

Proposition 4.10 – *Soit E un espace vectoriel euclidien. L'ensemble des endomorphismes orthogonaux est un sous groupe du groupe $GL(E)$.*

Démonstration : Exercice. ∎

Définition 4.11 – *Soit E un espace vectoriel euclidien. Le sous-groupe du groupe $GL(E)$ composé des endomorphismes orthogonaux est appelé le groupe orthogonal de E et est noté $O(E)$. On pose $SO(E) = O(E) \cap SL(E)$. Les éléments de $SO(E)$ sont appelés des rotations de E. Enfin, on pose $O^-(E) = O(E) \setminus SO(E)$.*

5 Etude du groupe orthogonal en dimension 2 et 3.

Soit E un espace vectoriel euclidien. Si $\mathcal{B}$ et $\mathcal{C}$ sont des bases orthonormales de E, la matrice P de passage de $\mathcal{B}$ à $\mathcal{C}$ est une matrice orthogonale. Sont déterminant est donc égal à 1 ou -1. Cette remarque permet de définir une orientation de l'espace. On se donne une base orthonormale de référence $\mathcal{B}$ de E (dont on dit qu'elle oriente E). On qualifie ensuite de directe (resp. indirecte) toute base orthonormale $\mathcal{C}$ de E telle que la matrice de passage de $\mathcal{B}$ à $\mathcal{C}$ soit (orthogonale et) de déterminant 1 (resp. -1).

A. Classification des isométries d'un espace vectoriel euclidien de dimension 2. On considère un espace vectoriel euclidien orienté E de dimension 2.

Exercice 5.1 – Soit P une matrice orthogonale de format 2×2.
1. On suppose que $\det(P) = 1$. Montrer qu'il existe un unique réel θ satisfaisant $0 \leq \theta < 2\pi$ et tel que

$$P = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

2. On suppose que $\det(P) = -1$. Montrer qu'il existe un unique réel θ satisfaisant $0 \leq \theta < 2\pi$ et tel que

$$P = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}.$$

Notation 5.2 – Pour tout réel θ, on pose :

$$R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \qquad \text{et} \qquad R'_\theta = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}.$$

Exercice 5.3 – On rappelle que E est un espace vectoriel euclidien de dimension 2. Montrer que $SO(E)$ est un groupe commutatif.

A.1 Le cas des rotations. On rappelle qu'une rotation de E est, par définition, une isométrie de déterminant 1.

Soit u une rotation de E. Etant donnée une base orthonormale directe $\mathcal{B}$ de E, d'après l'exercice 5.1, il existe un unique réel θ satisfaisant à $0 \leq \theta < 2\pi$ et tel que la matrice B de u relativement à $\mathcal{B}$ soit R_θ. Soit $\mathcal{C}$ une (autre) base orthonormale directe, soit P la matrice de passage de $\mathcal{B}$ à $\mathcal{C}$, C la matrice de u relativement à $\mathcal{C}$ et ϕ l'unique réel satisfaisant à $0 \leq \phi < 2\pi$ et tel que $C = R_\phi$. On a $C = P^{-1}BP$. Mais, d'après l'exercice 5.3, P et B commutent et il vient que $C = B$. On a donc montré qu'il existe un unique réel θ satisfaisant à $0 \leq \theta < 2\pi$ et tel que la matrice de u relativement à toute base orthonormale directe soit R_θ. Ce réel est appelé *la mesure d'angle* de la rotation u.

A.2 Le cas des isométries de déterminanat -1. Soit u une isométrie de E de déterminant -1. Etant donnée une base orthonormale $\mathcal{B}$ de E, d'après l'exercice 5.1, il existe un unique réel θ satisfaisant à $0 \leq \theta < 2\pi$ et tel que la matrice B de u relativement à $\mathcal{B}$ soit R'_θ. Il s'ensuit que le polynôme caractéristique de u est $X^2 - 1$ et que, par suite, u est diagonalisable. Plus précisément, il existe une base orthogonale (que l'on peut toujours choisir directe) relativement à laquelle la matrice de u est

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ainsi, u est une réflexion.

B. Classification des isométries d'un espace vectoriel euclidien de dimension 3. On considère un espace vectoriel euclidien orienté E de dimension 3.

Exercice 5.4 – On rappelle que E est un espace vectoriel euclidien de dimension 3. Montrer que tout élément de $O(E)$ admet 1 ou -1 pour valeur propre.

B.1. Le cas des rotations. On rappelle qu'une rotation de E est, par définition, une isométrie de déterminant 1.

Soit u une rotation de E. On commence par montrer que 1 est valeur propre de u. D'après l'exercice 5.4, il suffit de montrer que si -1 est valeur propre, alors 1 l'est aussi. Supposons donc que -1 est valeur propre de u et soit f_1 un vecteur propre de u (de norme 1) de valeur propre -1. On peut construire une base orthonormale $\{f_1, f_2, f_3\}$. La matrice de u relativement à cette base est de la forme

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}.$$

De plus, cette matrice étant orthogonale, sa matrice extraite construite sur les lignes et les colonnes $2, 3$ est aussi orthogonale. Comme elle est de déterminant -1, la classification des isométries en dimension 2 assure qu'elle admet 1 pour valeur propre et, par suite, que 1 est valeur propre de u. Il est facile de voir, alors, que la valeur propre 1 est de multiplicité 1 si $u \neq \mathrm{id}_E$.

Supposons dans la suite que $u \neq \mathrm{id}_E$. Fixons un vecteur propre f_1 de u (de norme 1 et) de valeur propre 1. En raisonnant comme pour la classification des isométries des espaces euclidiens de dimension 2, il est facile de voir qu'il existe un unique réel θ, satisfaisant $0 \leq \theta < 2\pi$ et tel que la matrice de u relativement à toute base orthonormale directe dont le premier vecteur est f_1 est

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

Ce réel est appelé *la mesure d'angle* de la rotation u *relatif au choix de* f_1 et $\mathbb{R}f_1$ est appelé l'axe de la rotation u.

B.2 Le cas des isométries de déterminant -1***.*** Soit u une isométrie de E de déterminant -1.

Par un raisonnement semblable à celui fait dans le cas des rotations, on montre que -1 est nécessairement valeur propre de u et que, de plus, la multiplicité de la valeur propre -1 est 1 si $u \neq -\mathrm{id}_E$.

Supposons dans la suite que $u \neq -\mathrm{id}_E$. Soit alors f_1 un vecteur propre de u de valeur propre -1 et de norme 1. En raisonnant comme pour la classification des rotations, il est facile de voir qu'il existe un unique réel θ, satisfaisant $0 \leq \theta < 2\pi$ et tel que la matrice de u relativement à toute base orthonormale directe dont le premier vecteur est f_1 est

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

Ce réel est appelé *la mesure d'angle* de u *relative au choix de* f_1 et $\mathbb{R}f_1$ est appelé l'axe de u.

Il est clair alors que u est la composée de la rotation ρ d'axe $\mathbb{R}f_1$ et de mesure d'angle θ relative au choix de f_1 et de la réflexion s par rapport à l'hyperplan $(\mathbb{R}f_1)^\perp$ et que, plus précisément, $u = \rho \circ s = s \circ \rho$.

6 *Exercices.*

§A - ***Exemples de produits scalaires ; propriétés élémentaires.***

Exercice 6.1 – On considère, sur $\mathbb{R}^2$, l'application $(.|.) : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ définie par

$$((x_1, x_2)|(y_1, y_2)) = x_1y_1 + x_2y_2 + \frac{1}{2}(x_1y_2 + x_2y_1).$$

Montrer que cette application définit un produit scalaire sur $\mathbb{R}^2$. Montrer que la base canonique de $\mathbb{R}^2$ n'est pas orthogonale pour ce produit scalaire et déterminer une base de $\mathbb{R}^2$ qui le soit.

Exercice 6.2 – On pose $E = \mathbb{R}_n[X]$. Soient $a_0, a_1, \ldots, a_n$ des éléments deux-à-deux distincts de $\mathbb{R}$. Montrer que l'application $(.|.) : E \times E \to \mathbb{R}$ définie par $(P|Q) = \sum_{j=0}^{n} P(a_j)Q(a_j)$ définit un produit scalaire sur E.

Exercice 6.3 – Soit k un réel. On considère, sur $\mathbb{R}^2$, l'application $(.|.) : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ définie par

$$((x_1, x_2)|(y_1, y_2)) = x_1y_1 + x_2y_2 + k(x_1y_2 + x_2y_1).$$

Quelles sont les valeurs de k pour lesquelles cette application définie un produit scalaire sur $\mathbb{R}^2$?

Exercice 6.4 – **Une autre identité de polarisation.** Soit $(E, (-,-))$ un espace vectoriel euclidien. Montrer que, pour tous $x, y \in E$, on a $4(x, y) = (||x + y||^2 - ||x - y||^2)$.

Exercice 6.5 – **Cas d'égalité de l'inégalité de Cauchy-Schwarz.** Soit $(E, (-,-))$ un espace vectoriel euclidien. Soient $x, y \in E$. Montrer que : $|(x, y)| = ||x||\,||y||$ si et seulement si x et y sont colinéaires.

Exercice 6.6 – **Cas d'égalité de l'inégalité triangulaire.** Soit $(E, (-,-))$ un espace vectoriel euclidien. Soient $x, y \in E$. Montrer que si $||x + y|| = ||x|| + ||y||$, alors x et y sont colinéaires. A-t-on la réciproque ?

§B - *Propriétés élémentaires liées à l'orthogonalité.*

Exercice 6.7 – Soit E un espace vectoriel euclidien et F un sous-espace vectoriel de E. Montrer que l'on a $(F^\perp)^\perp = F$.

Exercice 6.8 – On munit $\mathbb{R}_2[X]$ du produit scalaire défini, pour P et Q dans $\mathbb{R}_2[X]$, par $(P|Q) = \int_0^1 P(t)Q(t)dt$. Orthonormaliser la base $\{1, X, X^2\}$ de $\mathbb{R}_2[X]$.

Exercice 6.9 – Dans l'espace $\mathbb{R}^4$ muni de sa structure euclidienne standard on considère les vecteurs $v_1 = (1, 2, -1, -2)$, $v_2 = (2, 3, 0, -1)$, $v_3 = (5, -2, -5, -2)$ et $v_4 = (8, 10, -10, 4)$. Montrer que $\{v_1, v_2, v_3, v_4\}$ est une base de $\mathbb{R}^4$ et déterminer son orthonormalisée.

§C - *Endomorphismes symétriques, projections et symétries orthogonales.*

Exercice 6.10 – Soit u un endomorphisme symétrique de l'espace euclidien E. Montrer que si F est un sous-espace vectoriel de E stable sous u, alors $F^\perp$ est aussi stable sous u.

Exercice 6.11 – On se place dans l'espace vectoriel $\mathbb{R}^3$ muni de sa structure euclidienne standard. On considère l'endomorphisme $u : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ dont la matrice représentative dans la base canonique de $\mathbb{R}^3$ est

$$\begin{pmatrix} 4 & -2 & 2 \\ -2 & 7 & -4 \\ 2 & -4 & 7 \end{pmatrix}.$$

Montrer que u est symétrique. Diagonaliser u dans une base orthogonale.

Exercice 6.12 – Soit u est un endomorphisme de l'espace euclidien E. Monrer que les deux assertions suivantes sont équivalentes :
(i) u est symétrique ;
(ii) u est diagonalisable et les espaces propres de u sont deus-à-deux orthogonaux.

Exercice 6.13 – **Projections orthogonales.**
Soient E un espace vectoriel euclidien et u un projecteur de E (i.e. $u \in \mathcal{L}(E)$ et $u^2 = u$). Montrer que les assertions suivantes sont équivalentes :
(i) u est symétrique (i.e. $u^* = u$) ;
(ii) $\ker u = (\operatorname{Im} u)^\perp$.
Si u vérifie une des conditions ci-dessus on dit que u est la projection orthogonale sur $\operatorname{im} u$ parallèlement à $\ker u$.

Exercice 6.14 – L'espace vectoriel $\mathbb{R}^3$ est muni de sa structure euclidienne standard. Donner une expression explicite de la projection orthogonale sur l'hyperplan dont l'équation relativement à la base canonique de $\mathbb{R}^3$ est $x - y + 2z = 0$.

Exercice 6.15 – Décrire l'endomorphisme de $\mathbb{R}^3$ dont la matrice représentative dans la base canonique est $\begin{pmatrix} 1/6 & 1/3 & -1/6 \\ 1/3 & 2/3 & -1/3 \\ -1/6 & -1/3 & 1/6 \end{pmatrix}$.

Exercice 6.16 – **Symétries orthogonales, réflexions.**
Soit E une espace vectoriel euclidien.
1. On considère une symétrie s de E (*i.e.* $s \in \mathcal{L}(E)$ et $s^2 = \mathrm{id}$).
Montrer que les assertions suivantes sont équivalentes :
(i) s est un endomorphisme symétrique ;
(ii) s est un endomorphisme orthogonal ;
(iii) $\ker(s + \mathrm{id}_E) = \ker(s - \mathrm{id}_E)^\perp$.
Si s est une symétrie de E qui satisfait l'une des assertions ci-dessus, on dit que c'est la symétrie orthogonale par rapport à $\ker(s - \mathrm{id}_E)$.
2. On appelle réflexion de E toute symétrie orthogonale de E par rapport à un hyperplan.
Montrer qu'une symétrie orthogonale de E est une réflexion ssi il existe un vecteur non nul $v \in E$ tel que, pour tout $x \in E$,

$$s(x) = x - 2\frac{(x|v)}{(v|v)}v.$$

Exercice 6.17 – Dans l'espace vectoriel $\mathbb{R}^3$ muni de sa structure euclidienne standard, on considère l'endomorphisme dont la matrice dans la base canonique est

$$\frac{1}{9}\begin{pmatrix} 1 & 8 & 4 \\ 8 & 1 & -4 \\ 4 & -4 & 7 \end{pmatrix}.$$

Montrer que f est une réflexion.

Exercice 6.18 – On se place dans l'espace vectoriel $\mathbb{R}^3$ muni de sa structure euclidienne standard. On considère l'endomorphisme $u : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ dont la matrice représentative dans la base canonique de $\mathbb{R}^3$ est

$$\begin{pmatrix} -7 & 0 & 24 \\ 0 & 25 & 0 \\ 24 & 0 & 7 \end{pmatrix}.$$

Montrer que u est symétrique. Diagonaliser u dans une base orthogonale. En déduire une description *géométrique* de u.

Exercice 6.19 – Soit E une espace vectoriel euclidien. Montrer que, si u et v sont des vecteurs unitaires de E, il existe une réflexion et une seule qui envoie u sur v.

§D - *Distances d'un élément à un sous-espace.*

Exercice 6.20 – Soit E un espace vectoriel euclidien et F un sous-espace vectoriel de E.
1) Montrer que, pour tout x de E, il existe un élément y et un seul de F tel que $x - y \in F^{\perp}$. Montrer que $y = p(x)$, où p est la projection orthogonale sur F.
2) Avec les notations de 1), montrer que y est l'unique élément de F tel que $\|x-y\| = \inf_{t\in F}\{\|x-t\|\}$.

Exercice 6.21 – Soit E un espace vectoriel euclidien de dimension $n \in \mathbb{N}^*$ dont on note $(-|-)$ le produit scalaire. Soient p un entier tel que $1 \leq p \leq n$ et $x_1, \ldots, x_p \in E$. On note F le sous-espace vectoriel de E engendré par la famille $\{x_1, \ldots, x_p\}$, S la matrice $p \times p$ dont le coefficient d'indice (i, j), $1 \leq i, j \leq p$, est $(x_i|x_j)$. et $G(x_1, \ldots, x_p)$ le déterminant de S.
1. Soient $\mathcal{B}$ une base orthonormée de E et M la matrice $n \times p$ dont les colonnes sont les coordonnée de $x_1, \ldots, x_p$ dans la base $\mathcal{B}$. Montrer que l'on a ${}^tMM = S$.
2. On suppose que $p = n$. Montrer que l'on a $G(x_1, \ldots, x_n) \geq 0$. Montrer que $G(x_1, \ldots, x_n) > 0$ si et seulement si les vecteurs $x_1, \ldots, x_n$ sont linéairement indépendants.
3. En déduire que l'on a $G(x_1, \ldots, x_p) \geq 0$ et que $G(x_1, \ldots, x_p) > 0$ si et seulement si les vectreurs $x_1, \ldots, x_p$ sont linéairement indépendants.
4. On suppose que les vecteurs $x_1, \ldots, x_p$ sont linéairement indépendants. Soit $x \in E$. On note d la distance de x à F.
4.1 Soit y le projeté orthogonal de x sur F. Montrer que l'on a $G(x_1, \ldots, x_p, x) = G(x_1, \ldots, x_p, y) + d^2 G(x_1, \ldots, x_p)$.
4.2. En déduire que $d^2 = \dfrac{G(x_1, \ldots, x_p, x)}{G(x_1, \ldots, x_p)}$.

§E - *Endomorphismes orthogonaux.*

Exercice 6.22 – Soit E un espace vectoriel euclidien et u un endomorphisme orthogonal de E. Montrer que si u est diagonalisable, alors u est une symétrie orthogonale.

Exercice 6.23 – Décrire *géométriquement* les endomorphismes suivants de l'espace $\mathbb{R}^3$ donnés par leur matrice représentative dans la base canonique de $\mathbb{R}^3$:

$$\frac{1}{9}\begin{pmatrix} 8 & 1 & -4 \\ -4 & 4 & -7 \\ 1 & 8 & 4 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1/2 & 1/2 & -\sqrt{2}/2 \\ 1/2 & 1/2 & \sqrt{2}/2 \\ \sqrt{2}/2 & -\sqrt{2}/2 & 0 \end{pmatrix}, \quad \begin{pmatrix} 3 & 1 & -\sqrt{6} \\ 1 & 3 & \sqrt{6} \\ -\sqrt{6} & \sqrt{6} & -2 \end{pmatrix},$$

$$\begin{pmatrix} -3/5 & 4/5 & 0 \\ 0 & 0 & 1 \\ 4/5 & 3/5 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \frac{1}{3}\begin{pmatrix} 2 & -1 & 2 \\ -2 & -2 & 1 \\ -1 & 2 & 2 \end{pmatrix}, \quad \frac{1}{3}\begin{pmatrix} 1 & 2 & 2 \\ -2 & -1 & 2 \\ -2 & 2 & -1 \end{pmatrix}.$$

Exercice 6.24 – Dans $\mathbb{R}^3$, on considère la rotation r d'axe dirigé par $(1, -1, 2)$ et d'angle $2\pi/3$. Calculer la matrice de r dans la base canonique de $\mathbb{R}^3$.

Exercice 6.25 – On désigne par E l'espace $\mathbb{R}^2$ muni de sa structure d'espace vectoriel euclidien orienté standard. Montrer qu'il existe un morphisme surjectif de groupes $\mathbb{R} \longrightarrow SO(E)$ qui induit un isomorphisme de groupes entre $\mathbb{R}/2\pi\mathbb{Z}$ et $SO(E)$.

Exercice 6.26 – On désigne par E l'espace $\mathbb{R}^3$ muni de sa structure d'espace vectoriel euclidien orienté standard. Soit u un vecteur non nul de E et R la rotation vectorielle autour de $D = \mathbb{R}u$ et dont la mesure d'angle relative au choix de u est θ. Soit r une rotation vectorielle quelconque. Montrer que $r \circ R \circ r^{-1}$ est la rotation vectorielle autour de la droite $D' = \mathbb{R}(r(u))$ et de mesure d'angle θ. En déduire que $SO(E)$ n'est pas commutatif.

§F - *Engendrement du groupe orthogonal (dim. 2 et 3).*

Exercice 6.27 – On désigne par E l'espace $\mathbb{R}^2$ muni de sa structure d'espace vectoriel euclidien orienté standard. Soient u et v deux vecteurs unitaires. Montrer qu'il existe une rotation r et une seule telle que $v = r(u)$.

Exercice 6.28 – **Engendrement du groupe orthogonal en dimension 2.**
On désigne par E l'espace $\mathbb{R}^2$ muni de sa structure d'espace vectoriel euclidien orienté standard.
1. Montrer que la composée de deux réflexions est une rotation. On précisera la mesure d'angle de cette rotation en fonction des deux réflexions. (Indication : pour la seconde question, on pourra utiliser l'Exercice 6.27.)
2. Montrer que le groupe orthogonal de E est engendré par les réflexions.

Exercice 6.29 – **Engendrement du groupe orthogonal en dimension 3.**
On désigne par E l'espace $\mathbb{R}^3$ muni de sa structure d'espace vectoriel euclidien orienté standard.
1. Montrer que la composée de deux réflexions est une rotation. On précisera la mesure d'angle de cette rotation en fonction des deux réflexions. (Indication : on pourra s'inspirer des Exercices 6.27 et 6.28.)
2. Montrer que le groupe orthogonal de E est engendré par les réflexions.

§G - *Angles.*

Exercice 6.30 – **Angles orientés de vecteurs.** On désigne par E l'espace $\mathbb{R}^2$ muni de sa structure d'espace vectoriel euclidien orienté standard. On rappelle (cf. ex. 6.27) que, pour $u, v \in E$ unitaires, il existe une unique rotation r telle $v = r(u)$. On note alors $\widehat{(u,v)}$ cette unique rotation et on l'appelle l'angle orienté du couple (u, v). De plus, la mesure d'angle de $\widehat{(u,v)}$ (vu comme un élément de $\mathbb{R}/2\pi\mathbb{Z}$) est appelée la mesure d'angle orienté du couple (u, v) et est notée $\mathrm{mes}\widehat{(u,v)}$.
1. Soient u, v et w des vecteurs unitaires de E.
1.1. $\mathrm{mes}\widehat{(u,v)} = 0$ si et seulement si $u = v$;
1.2. $\mathrm{mes}\widehat{(u,v)} = \pi + 2\pi\mathbb{Z}$ si et seulement si $u = -v$;
1.3. $\mathrm{mes}\widehat{(u,v)} = \pm\pi/2 + 2\pi\mathbb{Z}$ si et seulement si u et v sont orthogonaux ;
1.3. $\mathrm{mes}\widehat{(u,v)} + \mathrm{mes}\widehat{(v,w)} = \mathrm{mes}\widehat{(u,w)}$ (relation de Chasles pour les angles) ;
1.4. $\mathrm{mes}\widehat{(u,v)} = -\mathrm{mes}\widehat{(v,u)}$.
2. Soient u et v des éléments de E, unitaires. Soit $g \in O^+(E)$. Montrer que

$$\mathrm{mes}\widehat{(g(u),g(v)} = \mathrm{mes}\widehat{(u,v)}$$

(On dit que les rotations conservent les mesures des angles orientés de vecteurs.)
3. Soit $f \in O^+(E)$ et $s \in O^-(E)$, montrer que $f^{-1} \circ s = s \circ f$. Soient u et v des éléments unitaires de E. Montrer que, pour $s \in O^-(E)$,

$$\text{mes}(\widehat{s(u), s(v)}) = -\text{mes}(\widehat{u, v})$$

(On dit que les réflexions transforment une mesure d'angle orienté de vecteurs en son opposé.)

Exercice 6.31 – **Angles orientés de vecteurs et fonctions trigonométriques.**
Pour aborder cet execice, le lecteur devra se référer aux notations de l'Exercice 6.30. Soient E un espace vectoriel orienté de dimension 2. On rappelle que le déterminant de deux vecteurs u et v de E est indépendant du choix de la base orthonormale directe dans lequel on le calcule ; on le note $\det(u, v)$. Soient u et v deux vecteurs unitaires de E.
1. Montrer que : $\cos(\text{mes}(\widehat{u, v})) = (u|v)$.
2. Montrer que : $\sin(\text{mes}(\widehat{u, v})) = \det(u, v)$.

Exercice 6.32 – **Angles orientés de droites.** On désigne par E l'espace $\mathbb{R}^2$ muni de sa structure d'espace vectoriel euclidien orienté standard. On rappelle que si d est une droite de E, il existe deux vecteurs unitaires opposés qui engendrent d. (Pour aborder cet execice, on conseille de consulter en détails l'Exercice 6.30.)
1. On note $\mathcal{D}$ l'ensemble des droites de E. Montrer qu'il existe une application

$$f \quad : \quad \mathcal{D} \times \mathcal{D} \quad \mapsto \quad O^+(E)/\{\pm \text{id}_{\overrightarrow{E}}\}$$

telle que, si u et v sont respectivement des vecteurs unitaires directeurs de d et δ, alors $f(d, \delta) = \widehat{(u, v)}\{\pm \text{id}_E\}$. Pour $d, \delta \in \mathcal{D}$, on pose $f(d, \delta) = \widehat{(d, \delta)}$.
2. Montrer que l'isomorphisme de groupes $\iota : O^+(E) \longrightarrow \mathbb{R}/2\pi\mathbb{Z}$ induit un isomorphisme de groupes $O^+(E)/\{\pm \text{id}_E\} \longrightarrow \mathbb{R}/\pi\mathbb{Z}$, que l'on note encore ι par abus de langage. On dispose donc d'une application

$$\mathcal{D} \times \mathcal{D} \quad \longrightarrow \quad O^+(E)/\{\pm \text{id}_E\} \quad \longrightarrow \quad \mathbb{R}/\pi\mathbb{Z} \ .$$

Si d et δ sont deux droites, on note $\text{mes}(\widehat{d, \delta})$ l'image du couple (d, δ) par l'application ci-dessus ; cet élément de $\mathbb{R}/\pi\mathbb{Z}$ est appelé mesure de l'angle orienté des droites d et δ.
3. Soient d et δ deux droites de E et u et v des vecteurs unitaires directeurs de d et δ, respectivement. On considère un réel α tel que $\text{mes}(\widehat{u, v}) = \alpha + 2\pi\mathbb{Z}$. Montrer qu'alors $\text{mes}(\widehat{d, \delta}) = \alpha + \pi\mathbb{Z}$.
4. Montrer les assertions suivantes. Pour toutes droites d_1, d_2, d_3 de E :
4.1. $\text{mes}(\widehat{d_1, d_2}) = 0$ si et seulement si $d_1 = d_2$;
4.2. $\text{mes}(\widehat{d_1, d_2}) + \text{mes}(\widehat{d_2, d_3}) = \text{mes}(\widehat{d_1, d_3})$;
4.3. $\text{mes}(\widehat{d_1, d_2}) = -\text{mes}(\widehat{d_2, d_1})$.

§G - *Produit vectoriel.*

Exercice 6.33 – **Produit vectoriel dans l'espace euclidien de dimension** 3.
0. *Question préliminaire.* Soit E un espace vectoriel euclidien de dimension finie $n \in \mathbb{N}^*$. On considère deux bases orthonormées directes $\mathcal{E}$ et $\mathcal{E}'$. Montrer que, si $a_1, \ldots, a_n$ sont des éléments de E, le déterminant dans $\mathcal{E}$ de la famille $\{a_1, \ldots, a_n\}$ coïncide avec le déterminant dans $\mathcal{E}'$ de la famille $\{a_1, \ldots, a_n\}$. On note $\det(a_1, \ldots, a_n)$ ce réel commun. On a donc défini une forme n-linéaire alternée

$$\begin{array}{ccc} E \times \ldots \times E & \longrightarrow & \mathbb{R} \\ a_1, \ldots, a_n & \mapsto & \det(a_1, \ldots, a_n) \end{array} .$$

1. Dans toute la suite, on note E l'espace vectoriel euclidien orienté $\mathbb{R}^3$ standard. On note $(-|-)$ son produit scalaire.
1.1. Soient x et y deux vecteurs fixés de E. On considère l'application

$$\begin{array}{rccc} \varphi & : & E & \longrightarrow & \mathbb{R} \\ & & z & \mapsto & \det(x,y,z) \end{array}.$$

Montrer que φ est une forme linéaire et en déduire qu'il existe un unique élément de E, noté $x \wedge y$, tel que

$$\det(x,y,z) = \varphi(z) = (x \wedge y|z), \quad \forall z \in E.$$

On dit que $x \wedge y$ est le produit vectoriel de x et y.
2. Soit $\mathcal{E} = \{e_1, e_2, e_3\})$ une base orthonormale directe de E. Soient $x, y \in E$. On pose $x = x_1e_1 + x_2e_2 + x_3e_3$ et $y = y_1e_1 + y_2e_2 + y_3e_3$. Montrer qu'alors

$$x \wedge y = (x_2y_3 - x_3y_2)e_1 + (x_3y_1 - x_1y_3)e_2 + (x_1y_2 - x_2y_1)e_3.$$

3. Soient $x, x', y \in E$ et $\lambda \in \mathbb{R}$. Montrer que l'on a :
(i) $y \wedge x = -(x \wedge y)$;
(ii) $x \wedge (\lambda y) = (\lambda x) \wedge y = \lambda(x \wedge y)$;
(iii) $(x + x') \wedge y = (x \wedge y) + (x' \wedge y)$.
4. Soient $x, y \in E$. Montrer que $x \wedge y = 0$ si et seulement si la famille $\{x, y\}$ est liée.
5. Soient $x, y \in E$. Montrer que $x \wedge y$ est orthogonal à x et y.
6. Soient $x, y \in E$ tels que $\{x, y\}$ soit libre. Montrer que $\{x, y, x \wedge y\}$ est une base de E et que le déterminant de cette famille dans toute base orthonormale directe de E est positif (*i.e.* $\{x, y, x \wedge y\}$ *est une base directe de* E).
7. Soit $\{x, y, z\}$ une base orthonormée directe. Montrer que $x \wedge y = z$, $y \wedge z = x$ et $z \wedge x = y$.

Exercice 6.34 – On note E l'espace vectoriel euclidien orienté $\mathbb{R}^3$ standard. Soit $r \in SO(E) \setminus \{\mathrm{id}\}$ une rotation d'axe $\mathbb{R}e$, avec $e \in E$ vecteur unitaire. On note θ la mesure d'angle de r relative au choix de e. Montrer que si u est un vecteur unitaire quelconque orthogonal à e, on a $u \wedge r(u) = \sin(\theta)e$.

Exercice 6.35 – **Produit vectoriel et endomorphismes antisymétriques.**
Un endomorphisme f d'un espace vectoriel euclidien E est dit antisymétrique si $f^* = -f$. Ceci est équivalent à dire que la matrice A de f dans une base orthonormale quelconque vérifie ${}^tA = -A$. On suppose dans la suite que E est un espace vectoriel euclidien orienté de dimension 3.
1. Soit $u \in E$. On considère l'application $f : E \longrightarrow E$ définie par : $f(x) = u \wedge x$ pour tout $x \in E$. Montrer que f est un endomorphisme antisymétrique de E.
2. Soit f un endomorphisme antisymétrique de E. Le but de cette question est de montrer qu'il existe un unique élément u de E tel que, pour tout $x \in E$, $f(x) = u \wedge x$.
2.1. Soit $\mathcal{B}$ une base orthonormée de E montrer qu'il existe des réels a, b, c tels que la matrice de f dans $\mathcal{B}$ soit :

$$\begin{pmatrix} 0 & -c & b \\ c & 0 & -a \\ -b & a & 0 \end{pmatrix}.$$

2.2. Soit $\mathcal{B}$ une base orthonormée de E et a, b, c les réels définis à la question 2.1. Soit en outre u le vecteur de E ayant pour coordonnées (a, b, c) dans la base $\mathcal{B}$. Montrer que, pour tout $x \in E$, $f(x) = u \wedge x$.
2.3. Conclure.

3. Soient $r \in O^+(E)$ et $f = r - r^*$. Montrer que f est un endomorphisme antisymétrique.
4. Soient $r \in O^+(E)$ et $f = r - r^*$. On suppose que $r^2 \neq Id_E$.
4.1. Soit u l'unique élément de E tel que, pour tout $x \in E$, $f(x) = u \wedge x$ (cf. questions 2 et 3). Montrer que l'axe de r est $\mathbb{R}u$.
4.2. Soit $\{e_1, e_2, e_3\}$ une base orthonormale directe dans laquelle la matrice de r est

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

Exprimer u en fonction de e_1.
5. Application.
Soit $f \in \mathcal{L}(\mathbb{R}^3)$ ayant pour matrice :

$$A = 1/3 \begin{pmatrix} 2 & 1 & 2 \\ -2 & 2 & 1 \\ -1 & -2 & 2 \end{pmatrix}$$

dans la base canonique de $\mathbb{R}^3$.
5.1. Montrer que $f \in O^+(\mathbb{R}^3)$.
5.2. En utilisant ce qui précède, déterminer l'axe de la rotation et la mesure de l'angle de la rotation.

§H - *Similitudes.*

Exercice 6.36 – **Similitudes.**
Soit E un espace vectoriel euclidien dont $(-,-)$ désigne le produit scalaire. Par définition, un endomorphisme de E est une similitude si il est de la forme λg où $\lambda \in \mathbb{R}_+^*$ et $g \in O(E)$. En outre, on dit qu'un endomorphisme u de E préserve l'orthogonalité si, pour tous $x, y \in E$, $(x, y) = 0$ implique que $(u(x), u(y)) = 0$. Il est clair que toute similitude préserve l'orthogonalité. Le but de la question 1 est de montrer que tout endomorphisme non nul qui préserve l'orthogonalité est une similitude.
1. Soit s un endomorphisme non nul qui préserve l'orthogonalité.
1.1. Soit z un élément non nul de E. Montrer qu'il existe un réel et un seul, λ_z, tel que, pour tout $x \in E$, $(s(x), s(z)) = \lambda_z(x, z)$.
Indication. Si $s(z) \neq 0$, on pourra s'intéresser aux formes linéaires $\phi = (-, z)$ et $\psi = (s(-), s(z))$ et montrer que leur noyau est l'hyperplan orthogonal à $\mathbb{R}z$ et en déduire qu'elles sont proportionnelles.
1.2. Montrer que si x et y sont des éléments de E non orthogonaux, alors $\lambda_x = \lambda_y$.
1.3. Montrer que si x et y sont des vecteurs non nuls de E et orthogonaux, alors $\lambda_x = \lambda_{x+y} = \lambda_y$.
1.4. Montrer que s est une similitude.
2. On considère un isomorphisme s de E tel que, pour tout $f \in O(E)$, $s \circ f \circ s^{-1} \in O(E)$.
2.1. Soit x un vecteur non nul de E. On note H l'hyperplan de E orthogonal à x. En considérant la réflexion par rapport à H, montrer que si un élément $y \in E$ est orthogonal à x, alors $s(y)$ est orthogonal à $s(x)$.
2.2. Montrer que s est une similitude.

Partie VIII

Géométrie affine.

Le corps de référence est le corps des nombres réels.

1 Structure d'espace affine.

Définition 1.1 – *Un espace affine est un triplet $(E, \overrightarrow{E}, \phi)$ où E est un ensemble non vide, $\overrightarrow{E}$ un $\mathbb{R}$-espace vectoriel et $\phi : E \times E \longrightarrow \overrightarrow{E}$, $(x, y) \mapsto \overrightarrow{xy}$ vérifiant les conditions suivantes :*
1. pour tous $x, y, z \in E$, $\overrightarrow{xy} + \overrightarrow{yz} = \overrightarrow{xz}$ (relation de Chasles) ;
2. pour tout $x \in E$, l'application $\phi_x : E \longrightarrow \overrightarrow{E}$, $y \mapsto \overrightarrow{xy}$, est bijective.

Par abus de langage, on parle de l'espace affine E. Les éléments de E sont appelés les points de E. On dit que $\overrightarrow{E}$ est la direction de l'espace affine E. On définit la dimension de E par $\dim E = \dim \overrightarrow{E}$.

Conformément aux habitudes, on appelle droite affine (resp. plan affine) un espace affine de dimension 1 (resp. 2).

Exercice 1.2 – Montrer que, pour tous $x, y \in E$, on a :
1. $\overrightarrow{xx} = \overrightarrow{0}$;
2. $\overrightarrow{xy} = -\overrightarrow{yx}$;
3. $\overrightarrow{xy} = \overrightarrow{0}$ entraîne $x = y$.

Chaque vecteur de $\overrightarrow{E}$ permet de définir une application de E dans E, appelée translation. C'est ce que l'on précise maintenant.

Remarque 1.3 –
1. Soit $\overrightarrow{u} \in E$. Compte tenu de la seconde condition dans la définition 1.1, à tout élément $x \in E$, on peut associer un élément y de E et un seul tel que $\overrightarrow{u} = \overrightarrow{xy}$ et on a $y = \phi_x^{-1}(\overrightarrow{u})$. On pose alors $y = x + \overrightarrow{u}$. Ainsi, on dispose d'une application

$$\begin{array}{rccc} T_{\overrightarrow{u}} & : & E & \longrightarrow & E \\ & & x & \mapsto & x + \overrightarrow{u} \end{array},$$

que l'on appelle la translation de vecteur $\overrightarrow{u}$.
2. On vérifie facilement que $T_{\overrightarrow{0}} = \mathrm{id}_E$. De plus, pour $\overrightarrow{u}$ et $\overrightarrow{v}$ dans E, $T_{\overrightarrow{u}+\overrightarrow{v}} = T_{\overrightarrow{u}} \circ T_{\overrightarrow{v}}$. Enfin, pour $\overrightarrow{u}$ dans E, $T_{\overrightarrow{u}}$ est bijective et sa bijection réciproque est $T_{-\overrightarrow{u}}$.
3. On peut alors considérer l'application

$$\begin{array}{ccc} E \times \overrightarrow{E} & \longrightarrow & E \\ (x, \overrightarrow{u}) & \mapsto & x + \overrightarrow{u} \end{array}.$$

On vérifie facilement que cette application définit une action (à droite) du groupe additif $(\overrightarrow{E}, +)$ sur l'ensemble E. C'est-à-dire que :
(i) pour tout $x \in E$, $x + \overrightarrow{0} = x$;
(ii) pour tout $x \in E$ et tous $\overrightarrow{u}, \overrightarrow{v}$ dans $\overrightarrow{E}$, $x + (\overrightarrow{u} + \overrightarrow{v}) = (x + \overrightarrow{u}) + \overrightarrow{v}$.
En outre, pour tous $x, y \in E$, il existe un vecteur $\overrightarrow{u}$ et un seul tel que $y = x + \overrightarrow{u}$ (avec les notation précédentes, on a $\overrightarrow{u} = \overrightarrow{xy}$).

Exercice 1.4 – Structure d'espace affine standard sur un espace vectoriel.
Soit E un espace vectoriel. Montrer que le triplet (E, E, ϕ), où $\phi : E \times E \longrightarrow E$, $(x, y) \mapsto x - y$, est un espace affine.

On présente maintenant l'exemple fondamental d'espace affine.

Exercice 1.5 – Soit $n \in \mathbb{N}^*$.
1. On sait que l'ensemble $\mathbb{R}^n$ est muni d'une structure naturelle de $\mathbb{R}$-espace vectoriel. On note $\overrightarrow{\mathbb{R}^n}$ ce $\mathbb{R}$-espace vectoriel. On considère l'application

$$\begin{array}{rccc} \phi & : & \mathbb{R}^n \times \mathbb{R}^n & \longrightarrow & \overrightarrow{\mathbb{R}^n} \\ & & ((a_1,\ldots,a_n),(b_1,\ldots,b_n)) & \mapsto & (b_1-a_1,\ldots,b_n-a_n) \end{array}.$$

Montrer que $(\mathbb{R}^n, \overrightarrow{\mathbb{R}^n}, \phi)$ est un espace affine.
2. Montrer que la structure d'espace affine ainsi définie sur $\mathbb{R}^n$ est la structure standard d'espace affine sur l'espace vectoriel $\overrightarrow{\mathbb{R}^n}$ (cf. exercice 1.4).

2 Barycentres et sous-espaces affines.

L'outil fondamental permettant l'étude des espaces affines est la notion de barycentre. Elle tient, dans le cadre affine, le rôle joué par la notion de combinaison linéaire dans le cadre vectoriel. Pour l'introduire, on a besoin de la notion de point pondéré. Un point pondéré de l'espace affine $(E, \overrightarrow{E}, \phi)$ est un couple (x, α) où x est un point de E et α un réel.

Théorème 2.1 – *Soient $p \in \mathbb{N}^*$ et $\{(a_1,\alpha_1),\ldots,(a_p,\alpha_p)\}$ une famille de p points pondérés de $E \times \mathbb{R}$. Si $\alpha_1 + \ldots + \alpha_p \neq 0$, il existe un unique point g de E tel que*

$$\alpha_1 \overrightarrow{ga_1} + \ldots \alpha_p \overrightarrow{ga_p} = \overrightarrow{0}.$$

Démonstration : Fixons un élément arbitraire $a \in E$. En outre, posons $\alpha = \alpha_1 + \ldots + \alpha_p \in \mathbb{R}^*$ et $\overrightarrow{u} = \alpha_1 \overrightarrow{aa_1} + \ldots \alpha_p \overrightarrow{aa_p}$. Il est facile de vérifier que le point $g = a + \dfrac{1}{\alpha}\overrightarrow{u}$ satisfait l'égalité requise. En outre, si g et h sont des points de E tels que $\alpha_1 \overrightarrow{ga_1} + \ldots \alpha_p \overrightarrow{ga_p} = \overrightarrow{0}$ et $\alpha_1 \overrightarrow{ha_1} + \ldots \alpha_p \overrightarrow{ha_p} = \overrightarrow{0}$, il est clair que l'on a $\overrightarrow{gh} = \overrightarrow{0}$, de sorte que $g = h$. ∎

Définition 2.2 – *Soient $p \in \mathbb{N}^*$ et $\{(a_1,\alpha_1),\ldots,(a_p,\alpha_p)\}$ une famille de p points pondérés de $E \times \mathbb{R}$. On suppose que $\alpha_1 + \ldots + \alpha_p \neq 0$. L'unique point g de E tel que*

$$\alpha_1 \overrightarrow{ga_1} + \ldots \alpha_p \overrightarrow{ga_p} = \overrightarrow{0}$$

(cf. théo. 2.1) est appelé le barycentre de la famille $\{(a_1,\alpha_1),\ldots,(a_p,\alpha_p)\}$.

Le barycentre d'un famille de points pondérés de E jouit de propriétés très agréables. L'exercice suivant dresse la liste des plus utiles.

Exercice 2.3 – Soient $p \in \mathbb{N}^*$ et $\{(a_1,\alpha_1),\ldots,(a_p,\alpha_p)\}$ une famille de p points pondérés de $E \times \mathbb{R}$. On suppose que $\alpha_1 + \ldots + \alpha_p \neq 0$. On note g le barycentre de cette famille.
1. Montrer que si l'on permute les points de la famille $\{(a_1,\alpha_1),\ldots,(a_p,\alpha_p)\}$, g reste inchangé.
2. Soit $\alpha \in \mathbb{R}^*$. Montrer que le barycentre de la famille $\{(a_1,\alpha\alpha_1),\ldots,(a_p,\alpha\alpha_p)\}$ est encore g.
3. Soit $q \in \mathbb{N}$ tel que $1 \leq q < p$. Supposons que $\alpha := \alpha_1 + \ldots + \alpha_q \neq 0$ et soit h le barycentre de $\{(a_1,\alpha_1),\ldots,(a_q,\alpha_q)\}$. Alors g est le barycentre de la famille $\{(h,\alpha),(a_{q+1},\alpha_{q+1}),\ldots,(a_p,\alpha_p)\}$.
4. Montrer qu'il existe des points a, b de E et des réels α, β de somme non nulle tels que g soit le barycentre de la famille $\{(a,\alpha),(b,\beta)\}$. (Attention : ce n'est pas tout-à-fait aussi simple qu'il n'y parait.)

Définition 2.4 – *Soient $p \in \mathbb{N}^*$ et $\{a_1, \ldots, a_p\}$ une famille de p points de E. On appelle isobarycentre de la famille $\{a_1, \ldots, a_p\}$ le barycentre de la famille $\{(a_1, 1), \ldots, (a_p, 1)\}$.*

Définition 2.5 – *Soient a_1 et a_2 deux points de E.*
1. On appelle milieu de a_1 et a_2 l'isobarycentre de la famille $\{a_1, a_2\}$.
2. On appelle segment d'extrémités a_1 et a_2 l'ensemble des points de E qui sont barycentre d'une famille pondérée $\{(a_1, \alpha_1), (a_2, \alpha_2)\}$ telle que $\alpha_1, \alpha_2 \in \mathbb{R}_+$ et $\alpha_1 + \alpha_2 \neq 0$.

On passe maintenant à la notion de sous-espace affine.

Définition 2.6 – Soient $(E, \overrightarrow{E})$ un espace affine et V une partie non vide de E. On dit que V est un sous-espace affine de E si elle est stable par barycentre, c'est-à-dire si elle satisfait à la condition suivante : pour tout $n \in \mathbb{N}$, toute famille $\{a_0, \ldots, a_n\}$ de points de V et toute famille $\{\alpha_0, \ldots, \alpha_n\}$ de réels tels que $\alpha_0 + \ldots + \alpha_n \neq 0$, le barycentre de la famille $\{(a_0, \alpha_0), \ldots, (a_n, \alpha_n)\}$ est un élément de V.

Le théorème 2.7 permet d'attacher un sous-espace vectoriel à tout sous-espace affine.

Théorème 2.7 – *Soient $(E, \overrightarrow{E})$ un espace affine, V une partie non vide de E.*
1. Soit $a \in V$. Les assertions suivantes sont équivalentes :
(i) V est un sous-espace affine de E ;
(ii) $\phi_a(V)$ est un sous-espace vectoriel de $\overrightarrow{E}$.
2. Soient $a, b \in V$. Si V est un sous-espace affine de E, alors $\phi_a(V) = \phi_b(V)$.

Démonstration : Rappelons que $\phi_a(V) = \{\overrightarrow{ax},\ x \in V\}$.
1. Montrons que (i) implique (ii). Il est clair que $\overrightarrow{0} = \phi_a(a) \in \phi_a(V)$. Soient $\overrightarrow{u}$ et $\overrightarrow{v}$ dans $\phi_a(V)$ et soit $\lambda \in \mathbb{R}$. Il existe x et y dans V tels que $\overrightarrow{u} = \overrightarrow{ax}$ et $\overrightarrow{v} = \overrightarrow{ay}$. Soit alors $z \in E$ tel que $\overrightarrow{az} = \overrightarrow{ax} + \overrightarrow{ay}$. On a alors $\overrightarrow{ax} + \overrightarrow{ay} - \overrightarrow{az} = \overrightarrow{0}$, ce qui s'écrit encore (via la relation de Chasles) $\overrightarrow{zx} + \overrightarrow{zy} - \overrightarrow{za} = \overrightarrow{0}$. Cette dernière égalité exprime que z est barycentre d'une famille de points de V, il est donc dans V et par suite $\overrightarrow{u} + \overrightarrow{v} \in \phi_a(V)$. On montre de la même façon que $\lambda\overrightarrow{u} \in \phi_a(V)$.
Montrons que (ii) implique (i). Soient $x, y \in V$ et α, β des réels tels que $\alpha + \beta \neq 0$. Soit enfin g le barycentre de $\{(x, \alpha), (y, \beta)\}$. On a $\alpha\overrightarrow{gx} + \beta\overrightarrow{gy} = \overrightarrow{0}$. Ce qui donne (par la relation de Chasles) $(\alpha + \beta)\overrightarrow{ga} + \alpha\overrightarrow{ax} + \beta\overrightarrow{ay} = \overrightarrow{0}$. Comme $\phi_a(V)$ est un sous-espace vectoriel, il s'ensuit que $\phi_a(g) = \overrightarrow{ag} \in \phi_a(V)$ puis, ϕ_a étant une bijection, que $g \in V$.
2. Soit $\overrightarrow{u} \in \phi_a(V)$. Il existe $x \in V$ tel que $\overrightarrow{u} = \overrightarrow{ax}$. Ainsi, $\overrightarrow{u} = \overrightarrow{ax} = \overrightarrow{ab} + \overrightarrow{bx} \in \phi_b(V)$. Ainsi, $\phi_a(V) \subseteq \phi_b(V)$. L'inclusion en sens inverse se montre de la même façon. ∎

Définition 2.8 – *Soient $(E, \overrightarrow{E})$ un espace affine et V un sous-espace affine de E. Le sous-espace vectoriel de $\overrightarrow{E}$ égal à $\phi_a(V)$ pour tout $a \in V$ (cf. théo. 2.7) s'appelle la direction de V et est noté $\overrightarrow{V}$.*

Remarque 2.9 – Soient $(E, \overrightarrow{E})$ un espace affine, V un sous-espace affine de E et $\overrightarrow{V}$ sa direction. Soit $a \in V$, arbitraire. D'après le théorème 2.7, on a $\overrightarrow{V} = \phi_a(V)$. Il s'ensuit que

$$V = \{a + \overrightarrow{u},\ \overrightarrow{u} \in \overrightarrow{V}\} = \{T_{\overrightarrow{u}}(a),\ \overrightarrow{u} \in \overrightarrow{V}\} =: a + \overrightarrow{V}.$$

Remarque 2.10 – Soient $(E, \overrightarrow{E}, \phi))$ un espace affine, V un sous-espace affine de E et $\overrightarrow{V}$ sa direction. Alors, $(V, \overrightarrow{V}, \phi')$ est un espace affine, où ϕ' est l'application de $V \times V$ dans $\overrightarrow{V}$ induite par ϕ.

Exercice 2.11 – Soit E un espace affine. Si V et W sont des espaces affines de même dimension finie et si l'un est inclus dans l'autre, alors ils sont égaux.

Définition 2.12 – *Soient E un espace affine de dimension $n \in \mathbb{N}^*$. Un hyperplan affine de E est un sous-espace affine de E de dimension $n-1$.*

Définition 2.13 – *Soient E un espace affine. Soient V et W des sous-espaces affines de E de directions respectives $\overrightarrow{V}$ et $\overrightarrow{W}$.*
1. On dit que V et W sont parallèles si $\overrightarrow{V} = \overrightarrow{W}$.
2. On dit que V et W sont faiblement parallèles si $\overrightarrow{V} \subseteq \overrightarrow{W}$ ou $\overrightarrow{V} \supseteq \overrightarrow{W}$.
3. On dit que V et W sont supplémentaires si $\overrightarrow{V}$ et $\overrightarrow{W}$ le sont.

Les sous-espaces affines rencontrés en pratique comme dans un cadre théorique sont souvent les *plus petits sous-espaces affines contenant* un ensemble donné de points de l'espace affine ambiant. On donne maintenant un sens précis à cette idée intuitive.

Théorème 2.14 – *Soient E un espace affine et $(V_i)_{i\in I}$ une famille de sous-espaces affines de E indexée par l'ensemble I non vide. Alors, si $\cap_{i\in I} V_i$ est non vide, c'est un sous-espace affine de E dont la direction est $\cap_{i\in I}\overrightarrow{V_i}$.*

Démonstration : Exercice. ∎

Définition 2.15 – *Soit E un espace affine.*
1. Soit A un sous-ensemble non vide de E. On appelle sous-espace affine engendré par A l'intersection de tous les sous-espaces affines de E contenant A. Le sous-espace affine engendré par A sera noté $\mathrm{Aff}(A)$.
2. Soit $\mathcal{F}$ une famille d'éléments de E indexée par un ensemble non vide I. On appelle sous-espace affine engendré par $\mathcal{F}$ le sous-espace affine de E engendré par le sous-ensemble de E sous-jacent à $\mathcal{F}$.

Remarque 2.16 – Soient E un espace affine et A un sous-ensemble non vide de E. Le sous-espace affine engendré par A contient A et est contenu dans tout sous-espace affine de E contenant A. En ce sens, il est le plus petit sous-espace affine de E contenant A.

La description suivante du sous-espace affine engendré par un sous-ensemble est à la fois plus parlante et plus utile dans la pratique.

Proposition 2.17 – *Soient E un espace affine et A un sous-ensemble non vide de E.*
1. Le sous-espace affine de E engendré par A est l'ensemble des points de E qui sont barycentres de familles de points de A pondérés.
2. Soit $a \in A$. La direction de $\mathrm{Aff}(A)$ *est le sous-espace vectoriel de $\overrightarrow{E}$ engendré par $\phi_a(A)$.*

Démonstration : On note B le sous-ensemble des points de E qui sont barycentres de familles de points de A pondérés. On a donc $A \subseteq B$ et par suite B est non vide.

Commençons par montrer que B est un sous-espace affine. Pour cela, fixons arbitrairement un élément $a \in A$. D'après le théorème 2.7, il suffit de montrer que $\phi_a(B)$ est un sous-espace vectoriel de $\overrightarrow{E}$.

Montrons que $\phi_a(B) = \mathrm{Vect}(\phi_a(A))$. Soit $g \in B$. Il existe $p \in \mathbb{N}^*$, $\alpha_1, \ldots, \alpha_p \in \mathbb{R}$ de somme égale à 1 et $x_1, \ldots, x_p \in A$ tels que g soit le barycentre de la famille $\{(x_1, \alpha_1), \ldots, (x_p, \alpha_p)\}$. On a donc $\alpha_1\overrightarrow{gx_1} + \ldots + \alpha_p\overrightarrow{gx_p} = \overrightarrow{0}$. Ce dont on déduit que $\phi_a(g) = \overrightarrow{ag} = \alpha_1\overrightarrow{ax_1} + \ldots + \alpha_p\overrightarrow{ax_p} \in$

$\mathrm{Vect}(\phi_a(A))$. Ainsi, $\phi_a(B) \subseteq \mathrm{Vect}(\phi_a(A))$. Réciproquement, soient $x_1, \ldots, x_p$ des éléments de A et $\lambda_1, \ldots, \lambda_p$ des réels ($p \in \mathbb{N}^*$). On veut montrer que $\sum_{i=1}^n \lambda_i \overrightarrow{ax_i} \in \phi_a(B)$. Soit $y \in E$ tel que $\overrightarrow{ay} = \sum_{i=1}^p \lambda_i \overrightarrow{ax_i}$. Il s'agit donc de montrer que $y \in B$. Mais, de $\overrightarrow{ay} = \sum_{i=1}^p \lambda_i \overrightarrow{ax_i}$, on tire que $(1 - \sum_{i=1}^p \lambda_i)\overrightarrow{ya} + \sum_{i=1}^p \lambda_i \overrightarrow{yx_i} = \overrightarrow{0}$, ce qui montre que $y \in B$. Donc $\phi_a(B) \supseteq \mathrm{Vect}(\phi_a(A))$.

Dans ce qui précède, on a montré que $\phi_a(B) = \mathrm{Vect}(\phi_a(A))$. D'après le théorème 2.7, ceci assure que B est un sous-espace affine. Comme il est clair que B est inclus dans tout sous-espace affine contenant A, on a bien $B = \mathrm{Aff}(A)$. ∎

Exemple 2.18 – Soit E un espace affine.
1. Si x, y sont des éléments distincts de E, $\mathrm{Aff}(\{x, y\})$ est une droite affine dont la direction est $\mathbb{R}\overrightarrow{xy} \subseteq \overrightarrow{E}$. On note (xy) cette droite affine.
2. Réciproquement, toute droite affine D de E contient deux éléments distincts et est engendrée par n'importe quel couple de points distincts qu'elle contient.

On explore maintenant les *sommes* de sous-espaces affines.

Théorème 2.19 – *(Théorème d'incidence.) Soient E est espace affine et V et W deux sous-espaces affines de E, de dimension finie.*
1. Si $V \cap W = \emptyset$, alors $\mathrm{Aff}(V \cup W)$ est un sous-espace affine de E de dimension $\dim(\overrightarrow{V} + \overrightarrow{W}) + 1$.
2. Si $V \cap W \neq \emptyset$, alors $\mathrm{Aff}(V \cup W)$ est un sous-espace affine de E de dimension $\dim(\overrightarrow{V} + \overrightarrow{W})$.

Démonstration : Exercice. ∎

Exercice 2.20 –
1. Soient E un espace affine de dimension 2 et D_1 et D_2 deux sous-espaces affines de E de dimension 1. Décrire $\mathrm{Aff}(D_1 \cup D_2)$.
2. Soient E un espace affine de dimension 3 et D_1 et D_2 deux sous-espaces affines de E de dimension 1. Décrire $\mathrm{Aff}(D_1 \cup D_2)$.

Exercice 2.21 –
1. Soient E un espace affine et V et W deux sous-espaces affines dont les directions sont des sous-espaces supplémentaires de $\overrightarrow{E}$. Montrer que $V \cap W$ n'est pas vide et que c'est un sous-espace affine de dimension 0.
2. Soient E un espace affine de dimension 3, P un plan de E et D une droite de E. Montrer qu'on est dans l'un des trois cas (complémentaires) suivants :
(i) $D \cap P = \emptyset$, et D et P sont faiblement parallèles,
(ii) $D \subset P$,
(iii) $D \cap P$ est un point.

A l'instar de la notion de base pour les espaces vectoriels, on peut définir la notion de *repère affine*. C'est à cette notion que l'on s'attache maintenant. On se limite au cas des espaces affines de dimension finie.

On commence par une proposition très utile dans la suite.

Proposition 2.22 – *Soient E un espace affine et $\{a_0, \ldots, a_k\}$ une famille de points de E ($k \in \mathbb{N}$). Le sous-espace affine engendré par la famille $\{a_0, \ldots, a_k\}$ est de dimension inférieure ou égale à k.*

Démonstration : Soit V le sous-espace affine engendré par $\{a_0, \ldots, a_k\}$. D'après la proposition 2.17, la direction de V est $\overrightarrow{V} = \mathrm{Vect}\{\overrightarrow{a_0a_1}, \ldots, \overrightarrow{a_0a_k}\}$. Le résultat s'ensuit aussitôt. ∎

Définition 2.23 – *Soit E un espace affine.*
1. Une famille de points de E est dite affinement génératrice si le sous-espace affine de E qu'elle engendre est E.
2. Une famille $\{a_0, \ldots, a_k\}$ de points de E ($k \in \mathbb{N}$) est dite affinement libre si le sous-espace de E qu'elle engendre est de dimension k.
3. Une famille $\{a_0, \ldots, a_k\}$ de points de E ($k \in \mathbb{N}$) est un repère affine si elle est affinement libre et affinement génératrice.

Exercice 2.24 – Soit E un espace affine. Soient $k \in \mathbb{N}^*$ et $\{a_0, \ldots, a_k\}$ une famille de points de E. Si a_0 est barycentre des points $a_1, \ldots, a_k$, alors $\{a_0, \ldots, a_k\}$ n'est pas affinement libre.

Proposition 2.25 – *Soit E un espace affine de dimension $n \in \mathbb{N}$.*
1. Si $\{a_0, \ldots, a_k\}$ est une famille de points de E qui est un repère affine, alors $k = n$.
2. Soit $\{a_0, \ldots, a_n\}$ une famille de points de E. Si $\{a_0, \ldots, a_n\}$ est affinement libre, elle est affinement génératrice.
3. Soit $\{a_0, \ldots, a_n\}$ une famille de points de E. Les assertions suivantes sont équivalentes :
(i) $\{a_0, \ldots, a_n\}$ est affinement libre ;
(ii) $\{a_0, \ldots, a_n\}$ est affinement génératrice ;
(iii) $\{a_0, \ldots, a_n\}$ est un repère affine.

Démonstration : 1. C'est clair.
2. Notons V le sous-espace affine engendré par $\{a_0, \ldots, a_n\}$. Par hypothèse, c'est un sous-espace affine de E de même dimension que E. L'exercice 2.11 assure alors que $V = E$, ce qui signifie que $\{a_0, \ldots, a_n\}$ est affinement génératrice (de E).
3. Cela découle immédiatement de ce qui précède. ∎

La notion de repère affine permet de repérer les points de E par des systèmes de coordonnées relatifs au repère choisi. Il faut bien prendre garde que, dans le cadre affine, un point admet plusieurs systèmes de coordonnées. On précise cela maintenant.

Remarque 2.26 – Soit E un espace affine de dimension n, $n \in \mathbb{N}$. Soit en outre $\{a_0, \ldots, a_n\}$ un repère affine de E.
1. Soit a un point de E. Puisque $\{a_0, \ldots, a_n\}$ est une famille affinement génératrice, il existe des scalaires $\alpha_0, \ldots, \alpha_n$ de somme non nulle tels que a soit barycentre de la famille $\{(a_0, \alpha_0), \ldots, (a_n, \alpha_n)\}$. Tout tel $(n+1)$-uplet est appelé un système de coordonnées barycentriques de a relativement au repère affine $\{a_0, \ldots, a_n\}$. Bien sûr, un tel $(n+1)$-uplet $(\alpha_0, \ldots, \alpha_n)$ n'est pas unique.
2. Soit a un point de E et si $(\alpha_0, \ldots, \alpha_n)$ et $(\beta_0, \ldots, \beta_n)$ sont deux systèmes de coordonnées barycentriques de a relativement au repère $\{a_0, \ldots, a_n\}$. En posant $\alpha = \sum_{i=0}^n \alpha_i$ et $\beta = \sum_{i=0}^n \beta_i$, on a alors

$$\alpha\overrightarrow{a_0 a} = \sum_{i=0}^{n} \alpha_i \overrightarrow{a_0 a_i} \quad \text{et} \quad \beta\overrightarrow{a_0 a} = \sum_{i=0}^{n} \beta_i \overrightarrow{a_0 a_i}.$$

Comme $\{a_0, \ldots, a_n\}$ est affinement libre, la famille $\{\overrightarrow{a_0 a_1}, \ldots, \overrightarrow{a_0 a_n}\}$ est une famille libre de E et il s'ensuit que, pour $0 \leq i \leq n$, $\alpha_i = \dfrac{\alpha}{\beta}\beta_i$. Ainsi, deux tels systèmes de coordonnées sont égaux à multiplication près par un scalaire non nul. Réciproquement, si $(\alpha_0, \ldots, \alpha_n)$ est un système de coordonnées affines pour a, tout n-uplet obtenu en le multipliant par un scalaire non nul est encore un système de coordonnées affines pour a.
3. Soit a un point de E. Il découle de ce qui précède qu'il existe un système $(\alpha_0, \ldots, \alpha_n)$ et un seul de coordonnées affines de a relativement à $\{a_0, \ldots, a_n\}$ tel que $\alpha_0 + \ldots + \alpha_n = 1$. Lorsqu'on

parlera *du* système de coordonnées affines de a par rapports à $\{a_0, \ldots, a_n\}$, c'est à celui-ci que l'on fera allusion.

L'exercice suivant établit un résultat utile dans la pratique.

Exercice 2.27 – Soient E un espace affine de dimension $n \in \mathbb{N}$ et $\mathcal{R} = \{a_0, \ldots, a_n\}$ un repère affine de E. On considère deux points x, y de E dont on note respectivement $(\alpha_0, \ldots, \alpha_n)$ et $(\beta_0, \ldots, \beta_n)$ le système de coordonnées barycentriques relativement à $\mathcal{R}$. Si λ est un réel et z le barycentre de la famille $\{(x, \lambda), (y, 1-\lambda)\}$, alors le système de coordonnées barycentriques de z par rapport à $\mathcal{R}$ est $(\lambda\alpha_0 + (1-\lambda)\beta_0, \ldots, \lambda\alpha_n + (1-\lambda)\beta_n)$.

On dispose également d'un second mode de repérage des points de E grâce à la notion de repère cartésien. Il repose sur l'observation suivante : si l'on fixe un point O de E, l'application $\phi_O : E \longrightarrow \overrightarrow{E}$ est un bijection. La donnée d'une base de $\overrightarrow{E}$ permet donc de repérer tout vecteur de $\overrightarrow{E}$ et donc, via ϕ_O, tout point de E.

Définition 2.28 – *Soit E un espace affine de dimension $n \in \mathbb{N}$. Un repère cartésien de E est la donnée d'un point $O \in E$ et d'une base $\{\overrightarrow{e_1}, \ldots, \overrightarrow{e_n}\}$ de $\overrightarrow{E}$. On note $R = (O, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ le repère ainsi défini. On appelle O l'origine du repère.*

Définition 2.29 – *Soient E un espace affine de dimension $n \in \mathbb{N}$ et $R = (O, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ un repère cartésien de E. Si m est un point de E, les coordonnées cartésiennes de m dans le repère R sont les coordonnées du vecteur $\overrightarrow{Om}$ de E relativement à la base $\{\overrightarrow{e_1}, \ldots, \overrightarrow{e_n}\}$ de $\overrightarrow{E}$.*

Le choix d'un repère cartésien de l'espace affine E permet de décrire les sous-espaces affines de E au moyen d'équations. C'est l'aspect que l'on développe maintenant. De même que tout sous-espace vectoriel d'un espace vectoriel peut être décrit comme intersection d'hyperplan de cet espace, tout sous-espace affine de E est intersection d'hyperplans affines de E. On commence donc par s'intéresser aux hyperplans affines. (Voir la définition 2.12.)

Soit E un espace affine de dimension $n \in \mathbb{N}^*$ et $R = (O, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ un repère cartésien de E.

Soit H un hyperplan affine de E, c'est-à-dire un sous-espace affine de E de dimension $n-1$. On note $\overrightarrow{H}$ la direction de H, de sorte que $\overrightarrow{H}$ est un hyperplan (vectoriel) de $\overrightarrow{E}$. Ainsi, il exite une forme linéaire (non nulle) $\overrightarrow{f} : \overrightarrow{E} \longrightarrow \mathbb{R}$ telle que $\overrightarrow{H} = \ker(\overrightarrow{f})$.

Soit a un élément quelconque de H. On a alors $\overrightarrow{H} = \phi_a(H)$. Et, un point m de E est dans H si et seulement si $\overrightarrow{am} = \phi_a(m) \in \overrightarrow{H}$. Finalement, on obtient que :

$$\forall\, m \in E,\ m \in H \Leftrightarrow \overrightarrow{f}(\overrightarrow{am}) = \overrightarrow{0}.$$

Ceci permet d'exprimer l'appartenance de m à H sous la forme d'une équation satisfaite par ses coordonnées cartésiennes dans le repère R. Pour cela, notons $(a_1, \ldots, a_n)$ les coordonnées cartésiennes de a dans $\mathbb{R}$. Si $(x_1, \ldots, x_n)$ sont les coordonnées cartésiennes du point m dans R, on a $\overrightarrow{am} = (x_1 - a_1)\overrightarrow{e_1} + \ldots + (x_n - a_n)\overrightarrow{e_n}$, et donc :

$$\overrightarrow{f}(\overrightarrow{am}) = (x_1 - a_1)\overrightarrow{f}(\overrightarrow{e_1}) + \ldots + (x_n - a_n)\overrightarrow{f}(\overrightarrow{e_n}).$$

Par suite, et avec ces notations, on a :

$$m \in H \Leftrightarrow (x_1 - a_1)\overrightarrow{f}(\overrightarrow{e_1}) + \ldots + (x_n - a_n)\overrightarrow{f}(\overrightarrow{e_n}) = 0.$$

On dit que l'expression ci-dessus est une équation cartésienne de H dans le repère R. Attention, une telle équation n'est pas unique puisque $\overrightarrow{f}$ n'est unique qu'à multiplication près par un scalaire non nul. En revanche, une fois choisi $\overrightarrow{f}$, le choix de a ne change pas l'équation. On laisse la vérification de ce fait en exercice. Ainsi, à multiplication près par un scalaire non nul, il existe une et une seule équation cartésienne de H dans R.

Passons maintenant au cas général où V est un sous-espace affine de E de dimension p ($0 \leq p < n$). Par définition de la dimension, la direction $\overrightarrow{V}$ de V est un sous-espace vectoriel de $\overrightarrow{E}$ de dimension p. Il s'ensuit que $\overrightarrow{V}$ est intersection de $n-p$ hyperplans vectoriels de $\overrightarrow{E}$. Plus précisément, il existe $n-p$ formes linéaires $\overrightarrow{f_1}, \ldots, \overrightarrow{f_{n-p}}$ de $\overrightarrow{E}^*$, linéairement indépendantes, et telles que $\overrightarrow{V} = \ker(\overrightarrow{f_1}) \cap \ldots \cap \ker(\overrightarrow{f_{n-p}})$. Soit alors a un point arbitrairement choisi dans V. Un point m de E est dans V si et seulement si $\overrightarrow{am}$ est dans $\overrightarrow{V}$. Il s'ensuit que, si $(x_1, \ldots, x_n)$ sont les coordonnées cartésiennes du point m dans R, on a

$$m \in V \Leftrightarrow \begin{cases} (x_1 - a_1)\overrightarrow{f_1}(\overrightarrow{e_1}) + \ldots + (x_n - a_n)\overrightarrow{f_1}(\overrightarrow{e_n}) = 0 \\ \qquad\qquad \vdots \qquad\quad \vdots \\ (x_1 - a_1)\overrightarrow{f_{n-p}}(\overrightarrow{e_1}) + \ldots + (x_n - a_n)\overrightarrow{f_{n-p}}(\overrightarrow{e_n}) = 0 \end{cases}.$$

3 Applications affines.

On aborde maintenant les application affines, c'est-à-dire les applications entre espaces affines qui préservent les structures de ces espaces.

Définition 3.1 – Soient E et F des espaces affines. Une application $f : E \longrightarrow F$ est dite affine si, pour tout $k \in \mathbb{N}^*$ et pour toute famille $\{(a_1, \alpha_1), \ldots, (a_k, \alpha_k)\}$ de points pondérés de E tels que $\alpha_1 + \ldots + \alpha_k \neq 0$, l'image du barycentre de $\{(a_1, \alpha_1), \ldots, (a_k, \alpha_k)\}$ par f est le barycentre de la famille $\{(f(a_1), \alpha_1), \ldots, (f(a_k), \alpha_k)\}$ de points pondérés de F.

A ce stade, il est utile d'introduire quelques notations. Soient $(E, \overrightarrow{E}, \phi)$ et $(F, \overrightarrow{F}, \psi)$ des espaces affines et $f : E \longrightarrow F$ une application. Soit en outre $a \in E$. Les application $\phi_a : E \longrightarrow \overrightarrow{E}$ et $\psi_{f(a)} : F \longrightarrow \overrightarrow{F}$ sont des bijections. On peut donc considérer l'application $f_a : \overrightarrow{E} \longrightarrow \overrightarrow{F}$ définie par $f_a = \psi_{f(a)} \circ f \circ \phi_a^{-1}$. Autrement dit, f_a est définie par :

$$\forall x \in E, \quad f_a(\overrightarrow{ax}) = \overrightarrow{f(a)f(x)}.$$

Bien sur, l'application f_a dépend de a. Cependant, on a le résultat suivant, qui permet de déterminer si une application est affine. (Voir le parallèle avec le théorème 2.7.)

Théorème 3.2 – *Soient E et F des espaces affines et $f : E \longrightarrow F$ un application.*
1. Soit $a \in E$. Les assertions suivantes sont équivalentes :
(i) f est affine ;
(ii) $f_a : \overrightarrow{E} \longrightarrow \overrightarrow{F}$ est linéaire.
2. Soient $a, b \in E$. Si f est affine, $f_a = f_b$.

Démonstration : On donne les grandes lignes. Les détails sont laissés en exercices.
1. Soit a dans E.
(i) implique (ii). On considère $x, y \in E$ et $\alpha, \beta \in \mathbb{R}$. Il existe $z \in E$ tel que $\overrightarrow{az} = \alpha\overrightarrow{ax} + \beta\overrightarrow{ay}$. Alors, z est barycentre de $\{(a, 1-\alpha-\beta), (x, \alpha), (y, \beta)\}$. Il s'ensuit que $f(z)$ est barycentre de

$\{(f(a), 1-\alpha-\beta), (f(x), \alpha), (f(y), \beta)\}$. On en déduit que $f_a(\overrightarrow{az}) = \alpha f_a(\overrightarrow{ax}) + \beta f_a(\overrightarrow{ay})$.
(ii) implique (i). Sans difficulté.
2. Sans difficulté. ∎

Remarque 3.3 – Soient E et F des espaces affines et $f : E \longrightarrow F$ un application affine. Il est facile de vérifier qu'il existe une unique application linéaire $\overrightarrow{f} : \overrightarrow{E} \longrightarrow \overrightarrow{F}$ telle que, pour tous $x, y \in E$, $\overrightarrow{f}(\overrightarrow{xy}) = \overrightarrow{f(x)f(y)}$ et que, pour tout $a \in A$, $\overrightarrow{f} = f_a$.

Définition 3.4 – *Soient $(E, \overrightarrow{E}, \phi)$ et $(F, \overrightarrow{F}, \psi)$ des espaces affines et $f : E \longrightarrow F$ une application affine. L'unique application linéaire $\overrightarrow{f} : \overrightarrow{E} \longrightarrow \overrightarrow{F}$ telle que, pour tous $x, y \in E$, $\overrightarrow{f}(\overrightarrow{xy}) = \overrightarrow{f(x)f(y)}$ (cf. théorème 3.2 et remarque 3.3) est appelée l'application linéaire associée à f.*

Remarque 3.5 – Soient E et F des espaces affines et $f : E \longrightarrow F$ une application affine d'application linéaire associée $\overrightarrow{f}$. Soit $a \in E$. Pour tout $x \in E$, on a

$$f(x) = f(a) + \overrightarrow{f}(\overrightarrow{ax}).$$

Exemple 3.6 – Premiers exemples d'applications affines.
Soit E un espace affine.
1. Translations. A tout vecteur $\overrightarrow{u}$ de $\overrightarrow{E}$ on associe l'application $T_{\overrightarrow{u}} : E \longrightarrow E$ introduite à la remarque 1.3. On vérifie facilement que $T_{\overrightarrow{u}}$ est une application affine. En effet, pour tout $a \in E$, $(T_{\overrightarrow{u}})_a = \mathrm{id}_{\overrightarrow{E}}$.

Notons que l'application id_E est donc une application affine puisque c'est la translation de vecteur nul.
2. Homothéties. Soit O un point de E et k un réel. On appelle homothétie de centre O et de rapport k l'application $h_{O,k}$, qui à $x \in E$ associe l'unique point y de E tel que $\overrightarrow{Oy} = k\overrightarrow{Ox}$. Alors, $h_{O,k}$ est une application affine dont l'application linéaire associée est $k\mathrm{id}_{\overrightarrow{E}}$. Il est clair que O est un point fixe de $h_{O,k}$.

Notons que l'homothétie de centre O et de rapport nul est l'application constante qui envoie tout point de E sur O. D'autre part, pour tout $O \in E$, l'homothétie de centre O et de rapport -1 est appelée symétrie centrale de centre O.

La proposition suivante est très utile dans la pratique.

Proposition 3.7 – *Soient E un espace affine et $f : E \longrightarrow E$ une application affine. On suppose qu'il existe $k \in \mathbb{R}$ tel que $\overrightarrow{f} = k.\mathrm{id}_{\overrightarrow{E}}$.*
1. Si $k = 1$, alors pour tous $x, y \in E$, $\overrightarrow{xf(x)} = \overrightarrow{yf(y)}$ et f est la translation de vecteur $\overrightarrow{af(a)}$, où a est un élément arbitraire de E.
2. Si f admet un point fixe O, alors f est l'homothétie de centre O et de rapport k.
3. Si $k \neq 1$, f admet un point fixe unique et si O est cet unique point fixe, f est l'homothétie de centre O et de rapport k.

Démonstration : Par hypothèse, pour tous $x, y \in E$, $\overrightarrow{f(x)f(y)} = \overrightarrow{f}(\overrightarrow{xy}) = k\overrightarrow{xy}$.
1. Du fait que $k = 1$, on tire que pour tous $x, y \in E$, $\overrightarrow{xf(x)} = \overrightarrow{yf(y)}$. Soit alors a un élément arbitraire de E, pour tout $x \in E$, on a $\overrightarrow{xf(x)} = \overrightarrow{af(a)}$, ce qui montre que f est la translation de vecteur $\overrightarrow{af(a)}$.
2. Puisque O est un point fixe de E, pour tout $x \in E$, on a $\overrightarrow{Of(x)} = k\overrightarrow{Ox}$, ce qui montre que f

est l'homothétie de centre O et de rapport k.
3. Soit a un point quelconque de E. Pour tout $x \in E$, on a $\overrightarrow{f(a)f(x)} = k\overrightarrow{ax}$. Ainsi, x est un point fixe de f si et seulement si $\overrightarrow{f(a)x} = k\overrightarrow{ax}$. Or, cette égalité équivaut à $\overrightarrow{f(a)a} = (k-1)\overrightarrow{ax}$. Comme $k \neq 1$, il est clair que cette dernière égalité admet une solution et une seule. On a donc montré que f admet un unique point fixe. Le reste se déduit du point 2. ∎

Les exercices suivants dressent la liste de quelques propriétés essentielles des applications affines.

Exercice 3.8 – Applications affines et sous-espaces affines.
Soient E et F des espaces affines et $f : E \longrightarrow F$ une application affine, dont on note $\overrightarrow{f}$ l'application linéaire associée. (On rappelle que, pour tout $a \in E$, $\overrightarrow{f} = \psi_{f(a)} \circ f \circ \phi_a^{-1}$.)
1. On a les assertions suivantes : f est injective si et seulement si $\overrightarrow{f}$ est injective ; f est surjective si et seulement si $\overrightarrow{f}$ est surjective ; f est bijective si et seulement si $\overrightarrow{f}$ est bijective.
2. Soit V un sous-espace affine de E de direction $\overrightarrow{V}$. Alors, $f(V)$ est un sous-espace affine de F de direction $\overrightarrow{f}(\overrightarrow{V})$.
3. Soit W un sous-espace affine de F de direction $\overrightarrow{W}$. Alors $f^{-1}(W)$ est soit vide soit un sous-espace affine de E de direction $\overrightarrow{f}^{-1}(\overrightarrow{W})$.
4. Si V et W sont des sous espaces affines parallèles (resp. faiblement parallèles) de E, alors $f(V)$ et $f(W)$ sont des sous espaces affines parallèles (resp. faiblement parallèles) de F.

Exercice 3.9 – Applications affines et composition.
1. Soient E, F, G des espaces affines, $f : E \longrightarrow F$ et $g : F \longrightarrow G$ des applications affines. Alors $g \circ f$ est une application affine d'application linéaire associée $\overrightarrow{g} \circ \overrightarrow{f}$.
2. Soient E, F des espaces affines et $f : E \longrightarrow F$ une application affine. Si f est bijective, alors $\overrightarrow{f}$ l'est aussi. De plus, $f^{-1} : F \longrightarrow E$ est une application affine dont l'application linéaire associée est $\overrightarrow{f}^{-1}$.

La proposition 3.11 est très utile dans la pratique. Elle permet de construire des applications affines.

Lemme 3.10 – *Soient E et F des espaces affines. Soient $a \in E$, $b \in F$ et $\bar{f} : \overrightarrow{E} \longrightarrow \overrightarrow{F}$ une application linéaire. Alors, il existe une unique application affine $f : E \longrightarrow F$ telle que $f(a) = b$ et dont l'application linéaire associée soit $\bar{f}$. De plus, pour tout $x \in E$, on a $f(x) = b + \bar{f}(\overrightarrow{ax})$.*

Démonstration : On considère l'application

$$\begin{array}{rccc} f & : & E & \longrightarrow & F \\ & & x & \mapsto & b + \bar{f}(\overrightarrow{ax}) \end{array} .$$

Il est immédiat que l'on a $f = \psi_b^{-1} \circ \bar{f} \circ \phi_a$. Il s'ensuit que f est affine (puisque $f_a = \bar{f}$ est linéaire). L'unicité se déduit facilement de la remarque 3.5. ∎

Proposition 3.11 – *Soit E un espace affine de dimension $n \in \mathbb{N}$ et F un espace affine. Si $\{a_0, \ldots, a_n\}$ est un repère affine de E et $\{b_0, \ldots, b_n\}$ une famille de points de F, il existe une application affine $f : E \longrightarrow F$ et une seule telle que, pour $0 \leq i \leq n$, $f(a_i) = b_i$.*

Démonstration : C'est une conséquence du lemme 3.10. Les détails sont laissés en exercice. ∎

4 Projections, symétries, affinités.

On décrit maintenant des applications affines particulièrement importantes : les projections, les symétries et les affinités.

Commençons par le cas des projections. Soit E un espace affine, V un sous-espace affine et $\overrightarrow{W}$ un sous-espace de $\overrightarrow{E}$ supplémentaire de $\overrightarrow{V}$ dans $\overrightarrow{E}$. Soit x un point de E. On sait que l'ensemble $(x+\overrightarrow{W}) = \{y \in E \,|\, \overrightarrow{xy} \in \overrightarrow{W}\}$ est un sous-espace affine de E, de direction $\overrightarrow{W}$. Il s'ensuit (d'après l'exercice 2.21) que $(x+\overrightarrow{W}) \cap V$ est un singleton. On peut donc poser la définition suivante.

Définition 4.1 – *Soit E un espace affine, V un sous-espace affine et $\overrightarrow{W}$ un sous-espace de $\overrightarrow{E}$ supplémentaire de $\overrightarrow{V}$ dans $\overrightarrow{E}$. On appelle projection sur V parallèlement à $\overrightarrow{W}$ l'application $p_{V,\overrightarrow{W}} : E \longrightarrow E$ qui à tout x de E associe l'unique élément de $(x+\overrightarrow{W}) \cap V$.*

Théorème 4.2 – On reprend les notations de la définition 4.1.
1. L'application $p_{V,\overrightarrow{W}}$ est une application affine dont l'application linéaire associée est la projection (vectorielle) de $\overrightarrow{E}$ sur $\overrightarrow{V}$ et parallèlement à $\overrightarrow{W}$.
2. Le sous-espace V est l'ensemble des points fixes de $p_{V,\overrightarrow{W}}$ ainsi que son image.
3. On a $p_{V,\overrightarrow{W}} \circ p_{V,\overrightarrow{W}} = p_{V,\overrightarrow{W}}$.

Démonstration : On pose $p = p_{V,\overrightarrow{W}}$.
Fixons $a \in V$. Il est clair que $p(a) = a$. Considérons alors $p_a = \phi_a \circ p \circ \phi_a^{-1}$. On doit montrer que p_a est linéaire. Soit $\overrightarrow{u}$ dans $\overrightarrow{E}$. Il existe un unique $x \in E$ tel que $\overrightarrow{u} = \overrightarrow{ax}$. Si l'on note y l'image de x par p, on a $y \in V$ et $\overrightarrow{xy} \in \overrightarrow{W}$. Bien sur, $\overrightarrow{ay} \in \overrightarrow{V}$. En outre, $\overrightarrow{u} = \overrightarrow{ax} = \overrightarrow{ay} + \overrightarrow{yx}$ est la décomposition de $\overrightarrow{u}$ suivant la somme directe $\overrightarrow{E} = \overrightarrow{V} \oplus \overrightarrow{W}$. Enfin, on vérifie facilement que $p_a(\overrightarrow{u}) = \overrightarrow{ay} \in \overrightarrow{V}$. Ceci prouve que p_a est la projection (vectorielle) sur $\overrightarrow{V}$, parallèlement à $\overrightarrow{W}$ qui est une application linéaire. Ceci prouve le premier points. Les autres points sont clairs.∎

Le théorème suivant caractérise les projections affines.

Théorème 4.3 – *Soit E un espace affine et $p : E \longrightarrow E$ une application affine. Les assertions suivantes sont équivalentes :*
(i) $p \circ p = p$;
(ii) $\overrightarrow{p} \circ \overrightarrow{p} = \overrightarrow{p}$ et p a un point fixe ;
(iii) il existe V sous-espace affine de E et $\overrightarrow{W}$ sous-espace de $\overrightarrow{E}$ supplémentaire de $\overrightarrow{W}$ dans $\overrightarrow{E}$ tels que $p = p_{V,\overrightarrow{W}}$.

Démonstration : (i) implique (ii). Comme $p \circ p = p$, on a bien $\overrightarrow{p} \circ \overrightarrow{p} = \overrightarrow{p}$. En outre, pour tout $x \in E$, $p(x)$ est un point fixe de p.
(ii) implique (iii). Comme $\overrightarrow{p} \circ \overrightarrow{p} = \overrightarrow{p}$, $\overrightarrow{p}$ est un projecteur de $\overrightarrow{E}$, de sorte que :

$$\overrightarrow{E} = \ker \overrightarrow{p} \oplus \operatorname{im} \overrightarrow{p}.$$

Soit a un point fixe de p. Posons $V = a + \operatorname{im}\overrightarrow{p}$ et $\overrightarrow{W} = \ker \overrightarrow{p}$. Nous allons montrer que p est la projection sur V, parallèlement à $\overrightarrow{W}$. Pour cela, il suffit de montrer que, pour tout $x \in E$, $p(x) \in (x+\overrightarrow{W}) \cap V$. Or, puisque a est un point fixe, $p = \phi_a^{-1} \circ \overrightarrow{p} \circ \phi_a$. Soit alors $x \in E$. L'observation ci-dessus montre que $\overrightarrow{ap(x)} = \overrightarrow{p}(\overrightarrow{ax}) \in \operatorname{im}\overrightarrow{p}$, et donc $p(x) \in V$. De plus, $\overrightarrow{xp(x)} = \overrightarrow{xa} + \overrightarrow{ap(x)} = \overrightarrow{xa} + \overrightarrow{p(a)p(x)} = \overrightarrow{xa} + \overrightarrow{p}(\overrightarrow{ax}) \in \overrightarrow{W}$. Donc, $p(x) \in x + \overrightarrow{W}$.

(iii) implique (i). Ceci est contenu dans le théorème 4.2. ∎

Poursuivons avec le cas des symétries.

Définition 4.4 – *Soient E un espace affine, V un sous-espace affine de E et $\overrightarrow{W}$ un sous-espace vectoriel de $\overrightarrow{E}$ supplémentaire de $\overrightarrow{V}$ dans $\overrightarrow{E}$. On appelle symétrie par rapport à V parallèlement à $\overrightarrow{W}$ l'application $s_{V,\overrightarrow{W}} : E \longrightarrow E$ qui à tout x de E associe l'unique élément $y \in E$ tel que $\overrightarrow{xy} = 2\overrightarrow{xz}$ où z est le projeté de x sur V parallèlement à $\overrightarrow{W}$.*

Théorème 4.5 – On reprend les notations de la définition 4.4.
1. L'application $s_{V,\overrightarrow{W}}$ est une application affine dont l'application linéaire associée est la symétrie (vectorielle) de $\overrightarrow{E}$ par rapport à $\overrightarrow{V}$ et parallèlement à $\overrightarrow{W}$.
2. Le sous-espace V est l'ensemble des points fixes de $s_{V,\overrightarrow{W}}$.
3. On a $s_{V,\overrightarrow{W}} \circ s_{V,\overrightarrow{W}} = \mathrm{id}_E$ (en particulier, $s_{V,\overrightarrow{W}}$ est bijective).

Démonstration : Exercice. ∎

Le théorème suivant caractérise les symétries affines.

Théorème 4.6 – *Soit E un espace affine et $s : E \longrightarrow E$ une application affine. Les assertions suivantes sont équivalentes :*
(i) $s \circ s = \mathrm{id}_E$;
(ii) $\overrightarrow{s} \circ \overrightarrow{s} = \mathrm{id}_{\overrightarrow{E}}$ et s a un point fixe ;
(iii) il existe V sous-espace affine de E et $\overrightarrow{W}$ sous-espace de $\overrightarrow{E}$ supplémentaire de $\overrightarrow{V}$ dans $\overrightarrow{E}$ tels que $s = s_{V,\overrightarrow{W}}$.

Démonstration : Exercice. ∎

On termine avec le cas des affinités.

Remarque 4.7 – Soit $\overrightarrow{E}$ un espace vectoriel, $\overrightarrow{V}$ et $\overrightarrow{W}$ deux sous-espaces vectoriels de $\overrightarrow{E}$, supplémentaires dans $\overrightarrow{E}$ et k un réel. On appelle affinité par rapport à $\overrightarrow{V}$, parallèlement à $\overrightarrow{W}$ et de rapport k l'unique application linéaire a de $\overrightarrow{E}$ telle que $a_{|\overrightarrow{V}}$ soit l'identité de $\overrightarrow{V}$ et $a_{|\overrightarrow{W}}$ soit l'homothétie de rapport k. Il est clair alors qu'un endomorphisme de $\overrightarrow{E}$ est une affinité si et seulement si il est diagonalisable et soit admet deux valeurs propres distinctes dont l'une est 1, soit admet une seule valeur propre. Enfin, avec les notations ci-dessus, si $k = 1$ a est l'identité, si $k = -1$ a est une symétrie, si $k = 0$ a est une projection et si $\overrightarrow{V} = \overrightarrow{0}$ a est un homothétie.

Définition 4.8 – *Soit E un espace affine, V un sous-espace affine de E, $\overrightarrow{W}$ un sous-espace de $\overrightarrow{E}$ supplémentaire de $\overrightarrow{V}$ dans $\overrightarrow{E}$ et k un réel. On appelle affinité par rapport à V parallèlement à $\overrightarrow{W}$ et de rapport k l'application $a_{V,\overrightarrow{W},k} : E \longrightarrow E$ qui à tout x de E associe l'unique élément $y \in E$ tel que $\overrightarrow{xy} = (1-k)\overrightarrow{xz}$ (c'est-à-dire $\overrightarrow{zy} = k\overrightarrow{zx}$) où z est le projeté de x sur V parallèlement à $\overrightarrow{W}$.*

Théorème 4.9 – On reprend les notations de la définition 4.8.
1. L'application $a_{V,\overrightarrow{W},k}$ est une application affine dont l'application linéaire associée est l'affinité (vectorielle) de $\overrightarrow{E}$ par rapport à $\overrightarrow{V}$, parallèlement à $\overrightarrow{W}$ et de rapport k.
2. Si $k \neq 1$, le sous-espace V est l'ensemble des points fixes de $a_{V,\overrightarrow{W},k}$.

Démonstration : Exercice. ∎

5 Le groupe affine.

On aborde maintenant l'étude d'un groupe important associé à tout espace affine : le groupe affine (de cet espace).

Définition 5.1 – *Soit E un espace affine. On appelle automorphisme affine de E toute application affine bijective de E dans E.*

Lemme 5.2 – *Soit E un espace affine. L'ensemble des automorphisme affine de E est sous-groupe du groupe des applications bijectives de E dans E muni de la loi de composition des applications. En particulier, l'ensemble des automorphismes affines est un groupe, dont le neutre est l'application identique.*

Démonstration : L'identité de E est un automorphisme affine (cf. 3.6). La composée de deux automorphismes affines est un automorphisme affine d'après l'exercice 3.9. La bijection réciproque d'un automorphisme affine est un automorphisme affine d'après l'exercice 3.9. ∎

Définition 5.3 – *Soit E un espace affine. Le groupe des automorphismes affines de E est appelé le groupe affine de E. Ce groupe sera noté $GA(E)$.*

Proposition 5.4 – *Soit $(E, \overrightarrow{E}, \phi)$ un espace affine.*
1. L'application linéaire associée à un automorphisme affine est un automorphisme de l'espace vectoriel $\overrightarrow{E}$ et l'application

$$\begin{array}{rccc} \Theta_E & : & GA(A) & \longrightarrow & GL(\overrightarrow{E}) \\ & & f & \mapsto & \overrightarrow{f} \end{array}$$

est un morphisme surjectif de groupes.
2. L'ensemble des translations de E, noté $T(E)$, est un sous-groupe normal de $GA(E)$ et c'est le noyau de Θ_E.

Démonstration : 1. Il résulte de l'exercice 3.9 que l'application linéaire associée à un automorphisme affine est un automorphisme de l'espace vectoriel $\overrightarrow{E}$ et que l'application Θ_E est un morphisme de groupes. En outre, le lemme 3.10 assure que Θ_E est surjectif.
2. D'après l'exercice 3.6 et la proposition 3.7, $\ker \Theta_E$ est l'ensemble des translations de E. Il en résulte que l'ensemble des translations de E est un sous-groupe normal de $GA(E)$. ∎

Remarque 5.5 – Soit E un espace affine. On reprend les notations de la proposition 5.4.
1. Le fait que $\ker \Theta_E$ soit l'ensemble des translations de E signifie que deux automorphismes affines f et g de E ont même application linéaire associée si et seulement si il existe une translation t de E telle que $g = f \circ t$ si et seulement si il existe une translation t' de E telle que $g = t' \circ f$.
2. Le fait que le sous-groupe $T(E)$ de $GA(E)$ soit normal signifie que, si t est une translation de E et g un automorphisme affine quelconque de E, alors $g^{-1} \circ t \circ g$ est une translation de E. (Plus précisément, si t est la translation de vecteur $\overrightarrow{u} \in \overrightarrow{E}$, alors $g^{-1} \circ t \circ g$ est la translation de vecteur $\overrightarrow{g}^{-1}(\overrightarrow{u})$).

Exercice 5.6 – On a déjà vu que l'ensemble des translations de E est un sous-groupe de $GA(E)$. Montrer qu'il est isomorphe au groupe $(\overrightarrow{E}, +)$.

Voici d'autres exemples importants de sous-groupes de E.

Exercice 5.7 – Soit E un espace affine. Soit O un point de E.
1. Montrer que l'ensemble H_O, des homothéties de centre O et de rapport non nul est un sous-groupe de $GA(E)$ isomorphe à $\mathbb{R}^*$.
2. Soit t la translation de E de vecteur $\overrightarrow{u}$ et h l'homothétie de E de centre O et de rapport $k \in \mathbb{R}^*$. Montrer que $t^{-1} \circ h \circ t$ est l'homothétie de centre $O' = O - \overrightarrow{u}$ et de rapport k. (On pourra utiliser l'exercice 3.6.) En déduire que H_O n'est pas normal dans $GA(E)$.

On considère maintenant un exemple plus intéressant.

On sait que l'ensemble $\mathcal{H} = \{k.\mathrm{id}_{\overrightarrow{E}},\ k \in \mathbb{R}^*\}$, des homothéties vectorielles de $\overrightarrow{E}$ de rapport non nul est un sous-groupe de $GL(E)$. En fait, c'est même son centre, et c'est donc un sous-groupe normal de $GL(\overrightarrow{E})$. On veut déterminer son image inverse par Θ_E. La proposition suivante va nous y aider.

Proposition 5.8 – *Soit E un espace affine et f un automorphisme affine de E. Les assertions suivantes sont équivalentes :*
(i) f est une homothétie ou une translation ;
(ii) $\overrightarrow{f}$ est un homothétie de rapport non nul.

Démonstration : (i) implique (ii). Cela se déduit immédiatement de l'exercice 3.6.
(ii) implique (i). Cela se déduit de la proposition 3.7. ∎

Corollaire 5.9 – *Soit E un espace affine. Le sous-ensemble de $GA(E)$ dont les éléments sont les homothéties et les translations de E est un sous-groupe normal de $GA(E)$.*

Démonstration : La proposition 5.8 montre que le sous-ensemble de $GA(E)$ dont les éléments sont les homothéties et les translations de E est l'image inverse par le morphisme de groupe Θ_E du sous-groupe normal $\mathcal{H}$ de $GL(\overrightarrow{E})$. A ce titre, c'est un sous-groupe normal de $GA(E)$. ∎

Remarque 5.10 – Soit E un espace affine. Il résulte du corollaire 5.9 que la composée d'une homothétie de rapport non nul et d'une translation ainsi que la composée de deux translations ou de deux homothéties de rapport non nul est une homothétie de rapport non nul ou une translation. Mais ce corollaire ne précise pas, en fonction du cas considéré, si la composée est une homothétie de rapport non nul ou si c'est une translation.

Définition 5.11 – *Soit E un espace affine. Le sous-ensemble de $GA(E)$ dont les éléments sont les homothéties et les translations de E est appelé le groupe de homothéties-translations. On le notera $HT(E)$.*

Le théorème suivant donne une autre caractérisation des éléments de $HT(E)$.

Proposition 5.12 – *Soit E un espace affine. Pour $f \in GA(E)$, les assertions suivantes sont équivalentes :*
(i) $f \in HT(E)$;
(ii) l'image de toute droite affine de E par f est une droite affine parallèle.

Démonstration : Les détails sont laissés en exercice. On pourra utiliser la proposition 5.8 et la seconde question de l'exercice 3.8.

On termine avec une famille de sous-groupes de $GA(E)$ qui sont isomorphes à $GL(\overrightarrow{E})$.

Proposition 5.13 – *Soit E un espace affine et O un point de E. L'ensemble des automorphismes affines dont O est un point fixe est un sous-groupe de $GA(E)$, isomorphe à $GL(\overrightarrow{E})$.*

Démonstration : On vérifie sans difficulté que l'ensemble G des automorphismes affines dont O est un point fixe est un sous-groupe de $GA(E)$. Le lemme 3.10 assure ensuite que la restriction de Θ_E à G est bijective. ∎

Définition 5.14 – *Soit E un espace affine et O un point de E. Le sous-groupe de $GA(E)$ des automorphismes affines dont O est un point fixe est appelé le sous-groupe stabilisateur de O. On le notera $GA_O(E)$.*

Exercice 5.15 – Soit E un espace affine et O un point de E.
1. Montrer que, pour toute automorphisme affine f de E, il existe un unique couple $(g,t) \in GA_O(E) \times T(E)$ tel que $f = t \circ g$.
2. Le sous-groupe $GA_O(E)$ est-il un sous-groupe normal de $GA(E)$?

6 *Exercices.*

Exercice 6.1 –
1. Soient $n, m \in \mathbb{N}^*$. On considère un système linéaire de m équations à n inconnues à coefficients dans $\mathbb{R}$. On suppose que ce système admet une solution dans $\mathbb{R}$. Montrer que l'ensemble des solutions de ce système dans $\mathbb{R}$ est un sous-espace affine de $\mathbb{R}^n$ et préciser sa direction.
2. On considère l'équation différentielle $y'' + 2y' + y = e^{2x}$. Montrer que l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ qui sont solutions de cette équation différentielle est un espace affine et préciser sa direction.

Exercice 6.2 – Médianes d'un triangle.
Soit E un espace affine de dimension 2 et soient A, B, C trois points non alignés de E. On appelle médiane issue de A du triangle (A,B,C) la droite engendrée par A et le milieu de $[BC]$, etc. Montrer que les trois médianes du triangle (A,B,C) sont concourantes.

Exercice 6.3 – Fonction vectorielle de Leibniz.
Soient E un espace affine, $n \in \mathbb{N}^*$ et $\{(a_1,\alpha_1),\ldots,(a_n,\alpha_n)\}$ une famille de points pondérés de E. On considère la fonction (dite fonction vectorielle de Leibniz associée à cette famille) :

$$\begin{array}{rccc} f & : & E & \longrightarrow & \overrightarrow{E} \\ & & m & \mapsto & \sum_{i=1}^p \alpha_i \overrightarrow{ma_i} \end{array}.$$

Montrer les assertions suivantes :
(i) si $\sum_{i=1}^p \alpha_i = 0$, alors f est une fonction constante ;
(ii) si $\sum_{i=1}^p \alpha_i \neq 0$, alors f est une fonction bijective.
Dans le second cas, expliciter f.

Exercice 6.4 – Soit E un espace affine. On considère quatre points A,B,C,D de E, distincts et tels qu'aucun de ces quatre points n'est sur la droite définie par deux quelconques des trois restants. On dit que (A,B,C,D) est un parallélogramme si $\overrightarrow{AB} = \overrightarrow{DC}$. Montrer que les assertions suivantes sont équivalentes :
(i) (A,B,C,D) est un parallélogramme ;
(ii) les milieux de $[AC]$ et $[BD]$ coïncident ;
(iii) (AB) est parallèle à (DC) et (AD) est parallèle à (BC).

Exercice 6.5 – Soient E un espace affine de dimension 2 et A, B, C trois points non alignés de E. On définit les points I, J, K, L, M, N de E par : $\overrightarrow{AI} = 1/3\overrightarrow{AB}$, $\overrightarrow{AJ} = 2/3\overrightarrow{AB}$, $\overrightarrow{BK} = 1/3\overrightarrow{BC}$, $\overrightarrow{BL} = 2/3\overrightarrow{BC}$, $\overrightarrow{AN} = 1/3\overrightarrow{AC}$, $\overrightarrow{AM} = 2/3\overrightarrow{AC}$. Montrer que les droites (IL), (JM) et (KN) sont concourantes en l'isobarycentre de (A, B, C).

Exercice 6.6 – Soit E un espace affine de dimension 2. On considère trois points A, B, C non alignés de E et trois réels a, b, c différents de 1. On considère en outre les 6 points suivants :
L, le barycentre de $\{(B, 1), (C, -a)\}$;
M, le barycentre de $\{(C, 1), (A, -b)\}$;
N, le barycentre de $\{(A, 1), (B, -c)\}$;
L', le barycentre de $\{(C, 1), (B, -a)\}$;
M', le barycentre de $\{(A, 1), (C, -b)\}$;
N', le barycentre de $\{(B, 1), (A, -c)\}$.
1. Montrer que L, M, N sont alignés si et seulement si $abc = 1$. Lorsque $abc = 1$, déterminer les réels d et e de somme 1 tels que L soit le barycentre de $\{(M, d), (N, e)\}$.
2. Montrer que, si L, M, N sont alignés sur une droite Δ, alors L', M', N' sont alignés sur une droite Δ' appelée isotomique de Δ par rapport au triangle (A, B, C).
3. Montrer que, si L, M, N sont alignés, les milieux de $[AL]$, $[BM]$, $[CN]$ sont alignés sur une droite parallèle à Δ'.

Exercice 6.7 – Soit E un espace affine de dimension $n \in \mathbb{N}$. Soit F un sous-espace affine de E de dimension p, $0 \leq p \leq n$. Montrer que si $\{b_0, \ldots, b_p\}$ est un repère affine de F, il existe des points $b_{p+1}, \ldots, b_n$ de E tels que $\{b_0, \ldots, b_n\}$ soit un repère affine de E.

Exercice 6.8 –
1. Soient E un espace affine de dimension $n \in \mathbb{N}$, $\mathcal{R}$ un repère affine de E et F un sous-espace affine de E de dimension p, $0 \leq p \leq n$ dont $\{b_0, \ldots, b_p\}$ est un repère affine. On pose

$$M_{\mathcal{R}}(\{b_0, \ldots, b_p\}) = (b_{ij})_{0 \leq i \leq n, 0 \leq j \leq p}.$$

Soit m un point de E dont on note $(m_0, \ldots, m_n)$ les coordonnées barycentriques de somme 1 dans $\mathbb{R}$. Montrer que m est dans F si et seulement si il existe $\alpha_0, \ldots, \alpha_p$ dans $\mathbb{R}$, de somme égale à 1 et tels que

$$\begin{pmatrix} m_0 \\ \vdots \\ m_n \end{pmatrix} = M_{\mathcal{R}}(\{b_0, \ldots, b_p\}) \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_p \end{pmatrix}.$$

Cette description des points de F s'appelle une *représentation paramétrique* de F relativement à $\mathcal{R}$.
2. Soit $E = \mathbb{R}^2$ muni de sa structure affine standard. On considère les points $A = (1, 0)$, $B = (0, 2)$ et $C = (2, 3)$. Déterminer une représentation paramétrique relativement au repère affine $\mathcal{R} = \{A, B, C\}$ de la droite de E engendrée par $X = (4, 0)$ et $Y = (3, 4)$.

Exercice 6.9 – Soit E un espace affine de dimension 3 et A, B, C, D quatre points non coplanaires de E. On note M_1 le milieu de $[AB]$, M_2 le milieu de $[BC]$, M_3 le milieu de $[CD]$ et M_4 le milieu de $[DA]$. Montrer que les points M_1, M_2, M_3 et M_4 engendrent un plan, que l'on note P. Montrer que les milieux de $[AC]$ et $[BD]$ ne sont pas dans le plan P.

Exercice 6.10 – Soient A, B, C, D quatre points non coplanaires d'une espace affine de dimension 3. On considère les points E, F, G tels que E soit le milieu de $[AB]$, $\overrightarrow{BF} = 2/3\overrightarrow{BC}$ et G soit

le barycentre de $\{(C,1),(D,3)\}$.
1. Donner les coordonnées barycentriques de E, F et G dans le repère affine $\mathcal{R}=\{A,B,C,D\}$.
2. En utilisant des coordonnées barycentriques, montrer qu'il existe un unique point H de (AD) tel que les droites (EG) et (HF) soient concourantes.

Exercice 6.11 – Dans le plan affine E, on considère 3 points A,B,C formant un repère affine $\mathcal{R}=\{A,B,C\}$ de E. On choisit trois points A', B' et C', appartenant respectivement aux droites (BC), (AC) et (AB), les points A, B et C étant exclus. On considère alors les réels α, β et γ, non nuls et différents de 1, tels que la matrice représentative de $\{A',B',C'\}$ dans $\mathcal{R}$ soit

$$\begin{pmatrix} 0 & \beta & 1-\gamma \\ 1-\alpha & 0 & \gamma \\ \alpha & 1-\beta & 0 \end{pmatrix}.$$

1. Donner une condition nécessaire et suffisante sur α et β pour que les droites (AA') et (BB') se coupent en un point unique M.
2. Donner une condition nécessaire et suffisante sur α, β et γ pour que les droites (AA'), (BB') et (CC') se coupent en un point unique M.
3. On suppose que la condition de la question 2 est réalisée. Montrer qu'on a alors (théorème de Gergonne) :

$$\frac{\overline{A'M}}{\overline{A'A}}+\frac{\overline{B'M}}{\overline{B'B}}+\frac{\overline{C'M}}{\overline{C'C}}=1.$$

Exercice 6.12 – On se place dans un espace affine E de dimension 3 rapporté au repère cartésien $R=(O,\vec{\imath},\vec{\jmath},\vec{k})$.
1. On note A le point de E dont les coordonnées dans R sont $(2,-1,0)$ et les vecteurs $\vec{u}$ et $\vec{u}'$ dont les coordonnées dans la base $(\vec{\imath},\vec{\jmath},\vec{k})$ de $\vec{E}$ sont respectivement $(-1,3,4)$ et $(2,-1,3)$. On note P le plan de direction $\mathrm{Vect}\{\vec{u},\vec{u}'\}$ contenant A. Soit D une droite contenue dans P et dont une équation cartésienne dans le repère $(A,\vec{u},\vec{u}'\}$ de P est $2X-3Y+6=0$. Déterminer une représentation paramétrique de D dans R, un repère cartésien $(B,\vec{v})$ de D et une représentation cartésienne de D dans R.
2. Déterminer des représentations paramétriques des sous-espaces affines engendrés par les familles suivantes de points de E :
(i) $(1,2,3)$, $(-1,3,1)$, $(7,-1,9)$,
(ii) $(1,2,3)$, $(-1,3,1)$, $(3,1,5)$,
(iii) $(1,2,3)$, $(-1,3,1)$, $(3,1,5)$, $(0,5,6)$,
(iv) $(1,2,3)$, $(-1,3,1)$, $(3,1,5)$, $(5,0,6)$.
On présisera leur dimension et on en donnera une représentation cartésienne.
3. Soit D la droite dont la représentation cartésienne dans R est :

$$\begin{cases} 5x-3y+z=0 \\ 2x+y-z+4=0 \end{cases}.$$

3.1. Donner une représentation paramétrique de D dans R et un reprère cartésien de D.
3.2. Soit D' la droite contenant le point de coordonnées $(-1,-2,0)$ dans R et dirigée par le vecteur de coordonnées $(3,-5,1)$ dans la base $(\vec{\imath},\vec{\jmath},\vec{k})$ de $\vec{E}$. Déterminer si D et D' sont parallèles, coplanaires et préciser leur intersection.
3.3. Soit Q le plan de E dont une représentation paramétrique dans R est

$$\begin{cases} x=2-4\alpha \\ y=-4+\alpha-\beta \\ z=1-2\alpha+4\beta \end{cases} ; \alpha,\beta\in\mathbb{R}.$$

Donner une équation cartésienne de Q. Déterminer si D est parallèle à Q ou non et préciser l'intersection de D et Q.

Exercice 6.13 – On se place dans un espace affine E de dimension 3 rapporté au repère cartésien $R = (O, \overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k})$.
On considère les points I, J, K de E définis par $OI = \overrightarrow{\imath}$, $OJ = \overrightarrow{\jmath}$ et $OK = \overrightarrow{k}$). On désigne par D la droite passant par O et K et par P le plan passant par O, I et J. En outre, on note D et D' les droites dont une représentation paramétrique dans R est, respectivement :

$$\begin{cases} x = 3 + \alpha \\ y = 9 - 4\alpha \\ z = \alpha \end{cases} ; \alpha \in \mathbb{R} \quad \text{et} \quad \begin{cases} x = 2 + 2\alpha \\ y = 4 + \alpha \\ z = \alpha \end{cases} ; \alpha \in \mathbb{R}.$$

1. Soit M le point de D défini par $\overrightarrow{OM} = \lambda \overrightarrow{k}$, $\lambda \in \mathbb{R}$. Le plan contenant M et parallèle à P coupe D' en M' et D'' en M''. Calculer, en fonction de λ, les coordonnées de M, M' et M'' dans R.
2. Déterminer λ pour que M, M' et M'' soient alignés.
3. En déduire qu'il existe deux droites Δ et Δ', parallèles à P et rencontrant D, D' et D''. Ecrire une représentation paramétrique de Δ et Δ' dans R.

Exercice 6.14 – On se place dans un espace affine E de dimension 2 rapporté au repère cartésien $R = (O, \overrightarrow{\imath}, \overrightarrow{\jmath})$.
Soit I un point de E. On appelle faisceau de droites de sommet I l'ensemble des droites de E passant par I.
1. Soient deux droites D et D' de E, distinctes, d'équations respectives $ux + vy + w = 0$ et $u'x + v'y + w' = 0$ et concourantes en I. Soit D'' une droite de E d'équation $u''x + v''y + w'' = 0$. Montrer que les assertions suivantes sont équivaentes :
(i) la droite D'' appartient au faisceau de somme I ;
(ii) $\det \begin{vmatrix} u & v & w \\ u' & v' & w' \\ u'' & v'' & w'' \end{vmatrix} = 0$;
(iii) il existe $\alpha, \beta \in \mathbb{R}$ tels que $u'' = \alpha u + \beta u'$, $v'' = \alpha v + \beta v'$ et $w'' = \alpha w + \beta w'$.
2. A tout réel m, on associe la droite D_m de E, d"equation

$$(m + 2)x + (2m - 1)y - m + 3 = 0.$$

2.1. Montrer que toutes les droites D_m, $m \in \mathbb{R}$, passent par un point I dont un précisera les coordonnées dans R.
2.2. L'ensemble $\{D_m, m \in \mathbb{R}\}$ coïncide-t-il avec le faisceau de droites de sommet I ?
2.3. Montrer que pour tout point M de E, distincts de I, il existe une et une seule droite du faisceau de droites de sommet I passant par M.

Exercice 6.15 – **Théorème de Thalès.**
Soit E un espace affine de dimension $n \in \mathbb{N}$. On considère trois hyperplans affines, H_1, H_2 et H_3 de E, deux-à-deux distincts et de même direction $\overrightarrow{H}$. On considère en outre deux droites D et D' non parallèles aux hyperplans précédants. Pour $i = 1, 2, 3$, on note A_i (resp. A'_i) l'intersection de D (resp. D') avec H_i. Montrer que les points A_1, A_2 et A_3 (resp. A'_1, A'_2 et A'_3) sont deux à deux distincts et que l'on a :

$$\frac{\overline{A_1A_2}}{\overline{A_1A_3}} = \frac{\overline{A'_1A'_2}}{\overline{A'_1A'_3}}.$$

Indication. On pourra utiliser une projection judicieusement choisie.

Exercice 6.16 – **Théorème de Ménélaüs.**
Soient E un espace affine et A, B, C trois points de E, non alignés. On considère trois points A', B', C' de E, distincts de A, B et C et tels que $A' \in (BC)$, $B' \in (AC)$ et $C' \in (AB)$. Montrer que A', B' et C' sont alignés si et seulement si

$$\frac{\overline{A'B}}{\overline{A'C}} \frac{\overline{B'C}}{\overline{B'A}} \frac{\overline{C'A}}{\overline{C'B}} = 1.$$

Indication. On pourra utiliser le repère affine $\{A, B, C\}$.

Exercice 6.17 – **Théorème de Ceva.**
Soient E un espace affine et A, B, C trois points de E, non alignés. On considère trois points A', B', C' de E, distincts de A, B et C et tels que $A' \in (BC)$, $B' \in (AC)$ et $C' \in (AB)$. Montrer que les droites (AA'), (BB') et (CC') sont parallèles ou concourantes si et seulement si

$$\frac{\overline{A'B}}{\overline{A'C}} \frac{\overline{B'C}}{\overline{B'A}} \frac{\overline{C'A}}{\overline{C'B}} = -1.$$

Indication. On pourra utiliser le repère cartésien $\{A, \overrightarrow{AB}, \overrightarrow{AC}\}$.

Exercice 6.18 – Soit E un espace affine de direction $\overrightarrow{E}$ et $f : E \longrightarrow E$ une application affine. On note $\mathrm{Fix}(f)$ l'ensemble des points fixes de f : $\mathrm{Fix}(f) = \{m \in E \mid f(m) = m\}$.
1. Montrer que $\mathrm{Fix}(f)$ est soit vide soit un sous-espace affine de E de direction $\ker\left(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}\right)$.
2. On suppose E de dimension finie. Montrer que les assertions suivantes sont équivalentes :
(i) f admet un point fixe et un seul ;
(ii) $\ker\left(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}\right) = \{\overrightarrow{0}\}$.

Exercice 6.19 – Soit E un espace affine de dimension 2, A, B, C des points de E non alignés et α, β, γ des réels tels que $\alpha + \beta + \gamma + 1 \neq 0$. On considère l'application $f : E \longrightarrow E$ qui à un point M de E associe le barycentre de $\{(A, \alpha), (B, \beta), (C, \gamma), (M, 1)\}$. Montrer que f est une homothétie ou une translation.

Exercice 6.20 – Soit E un espace affine. On sait que l'ensemble des homothéties de rapport non nul et des translations de E forme en groupe, que l'on note $HT(E)$. Il s'ensuit que si f et g sont des homothéties de rapport non nul ou des translations, la composée $f \circ g$ est une homothétie de rapport non nul ou une translation. Le but de cet exercice est de préciser, suivant les cas, si $f \circ g$ est une homothétie de rapport non nul ou une translation et de préciser laquelle.
1. Soient t et s deux translations de E. Décrire $t \circ s$.
2. Soient h une homothétie de centre $O \in E$ et de rapport non nul $k \neq 1$ et t une translation de vecteur $\overrightarrow{u} \in \overrightarrow{E}$, décrire $h \circ t$.
3. Soient h une homothétie de centre $O \in E$ et de rapport non nul $k \neq 1$ et t une translation de vecteur $\overrightarrow{u} \in \overrightarrow{E}$, décrire $t \circ h$.
4. Soient h une homothétie de centre $O \in E$ et de rapport non nul k et h' une homothétie de centre O' et de rapport non nul k', décrire $h \circ h'$.

Exercice 6.21 – **Le théorème de Ménélaüs par les homothéties.**
Soient E un espace affine de dimension 2 et A, B, C trois points non alignés de E. On considère trois points A', B' et C' de E, distincts de A, B et C tels que A' soit sur la droite (BC), B' soit sur la droite (AC) et C' soit sur la droite (AB). On définit les trois homothéties suivantes :

(i) h_1 est l'homothétie de centre A' et de rapport $\dfrac{\overline{A'B}}{\overline{A'C}}$;
(ii) h_2 est l'homothétie de centre B' et de rapport $\dfrac{\overline{B'C}}{\overline{B'A}}$;
(iii) h_3 est l'homothétie de centre C' et de rapport $\dfrac{\overline{C'A}}{\overline{C'B}}$.
1. Calculer $h_1(C)$, $h_2(A)$ et $h_3(B)$.
2. On suppose que A', B' et C' sont alignés. Montrer que $h_1 \circ h_2 \circ h_3 = \mathrm{id}_E$. En déduire que

$$\frac{\overline{A'B}}{\overline{A'C}}\frac{\overline{B'C}}{\overline{B'A}}\frac{\overline{C'A}}{\overline{C'B}} = 1.$$

3. On suppose que

$$\frac{\overline{A'B}}{\overline{A'C}}\frac{\overline{B'C}}{\overline{B'A}}\frac{\overline{C'A}}{\overline{C'B}} = 1.$$

Montrer que $h_1 \circ h_2 \circ h_3 = \mathrm{id}_E$. En déduire que A', B' et C' sont alignés.

Exercice 6.22 – Soient E un espace affine de dimension 3 et $R = (O, \overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k})$ un repère cartésien de E. On considère l'application $f : E \longrightarrow E$ qui à tout point M de coordonnées (x, y, z) dans R associe le point de coordonnées $(-4x - 2y + z - 7, x - y - z - 1, -3x - 6y - 9)$ dans R.
1. Montrer que f est une application affine bijective et expliciter sa partie linéaire $\overrightarrow{f}$.
2. Déterminer les valeurs propres et les sous-espaces propres de $\overrightarrow{f}$.
3. Montrer que f admet une droite de points fixes, que l'on notera Δ.
4. Décrire f géométriquement.

Exercice 6.23 – Soient E un espace affine de dimension 3 et $R = (O, \overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k})$ un repère cartésien de E. On considère les droites D et D' de E dont les représentations paramétriques dans R sont, respectivement :

$$\begin{cases} x &= 3 + t \\ y &= 9 - 4t \ , \ t \in \mathbb{R} \\ z &= t \end{cases} \qquad \text{et} \qquad \begin{cases} x &= 2 + 2u \\ y &= 4 + u \ , \ u \in \mathbb{R}. \\ z &= u \end{cases}$$

1. Montrer que le sous-espace affine P engendré par D et D' est un plan et en donner une équation cartésienne dans R.
2. Donner l'expression de l'image d'un point M de coordonnées (x, y, z) dans R par la projection sur P parallèlement à la droite $\mathbb{R}(\overrightarrow{i} + \overrightarrow{j} + \overrightarrow{k})$.
3. Donner l'expression de l'image d'un point M de coordonnées (x, y, z) dans R par la symétrie par rapport à P parallèlement à la droite $\mathbb{R}(\overrightarrow{i} + \overrightarrow{j} + \overrightarrow{k})$.

Exercice 6.24 – Soit E un espace vectoriel et V une partie de E. On munit E de sa structure canonique d'espace affine. Montrer que les assertions suivantes sont équivalentes :
(i) V est un sous-espace vectoriel de E ;
(ii) V est un sous-espace affine de E qui contient $\{0\}$.

Exercice 6.25 – Forme canonique des applications affines de $\mathbb{R}^q$ dans $\mathbb{R}^p$. Structure des ensembles de solutions des systèmes linéaires non homogènes.

Partie IX

Géométrie affine euclidienne.

1 Espaces affines euclidiens.

Définition 1.1 – *Un espace affine euclidien est la donnée d'un espace affine $(E, \overrightarrow{E}, \phi)$ sur $\mathbb{R}$ et d'une forme bilinéaire symétrique $(-|-) : \overrightarrow{E} \times \overrightarrow{E} \longrightarrow \mathbb{R}$ munissant $\overrightarrow{E}$ d'une structure d'espace euclidien.*

Remarque 1.2 – Par définition, un espace affine euclidien est de dimension finie (puisque tel est le cas d'un espace vectoriel euclidien).

Définition 1.3 – Soit E un espace affine euclidien de dimension $n \in \mathbb{N}$.
1. Un repère $(O, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ de E est dit orthonormé (direct) si la base $\{\overrightarrow{e_1}, \ldots, \overrightarrow{e_n}\}$ de $\overrightarrow{E}$ est orthonormée (directe).
2. Deux sous-espaces affines de E sont dits orthogonaux si leurs directions sont des sous-espaces vectoriels orthogonaux de $\overrightarrow{E}$.
3. Deux sous-espaces affines de E sont dits supplémentaires orthogonaux si leurs directions sont des sous-espaces vectoriels supplémentaires orthogonaux de $\overrightarrow{E}$.

Exercice 1.4 – Soit E un espace affine euclidien. Si V est un sous-espace affine de E et a un point de V, il existe un unique sous-espace affine de E, supplémentaire orthogonal de V et passant par a.

Du fait que $\overrightarrow{E}$ est un espace vectoriel normé (par la norme associée au produit scalaire $(-|-)$), E est un espace métrique. C'est l'objet de la proposition suivante. On note $||-||$ la norme euclidienne attachée à $(-|-)$.

Proposition 1.5 – *Soit E un espace affine euclidien. L'application*

$$\begin{array}{rccc} d & : & E \times E & \longrightarrow & \mathbb{R} \\ & & (x, y) & \mapsto & ||\overrightarrow{xy}|| \end{array}$$

est une distance sur E. Ainsi, (E, d) est un espace métrique.

Démonstration : Exercice. ∎

Exercice 1.6 – Soit E un espace affine euclidien dont on note d la distance.
1. Soit $\overrightarrow{u} \in \overrightarrow{E}$. Montrer que, pour tous $x, y \in E$, $d(T_{\overrightarrow{u}}(x), T_{\overrightarrow{u}}(y)) = d(x, y)$.
2. Soit $O \in E$, $k \in \mathbb{R}$ et h l'homothétie de centre O est rapport k. Montrer que, pour tous $x, y \in E$, $d(h(x), h(y)) = |k| d(x, y)$.
3. Soient $x, y, z \in E$. Montrer que $d(x, y) = d(x, z) + d(zy)$ si et seulement si $z \in [x, y]$. (On pourra utiliser le cas d'égalité dans l'inégalité de Minkovski.)

On peut également définir la distance entre deux parties non vides de E. A ce sujet, on rappelle que toute partie non vide et minorée de $\mathbb{R}$ admet une borne inférieure, ce qui permet de définir cette notion.

Définition 1.7 – *Soit E un espace affine euclidien dont on note d la distance.*
1. Si X et Y sont deux parties non vides de E, on définit la distance, $d(X, Y)$, entre X et Y, par

$$d(X, Y) = \inf\{d(x, y),\ x \in X,\ y \in Y\}.$$

2. Si x est un élément de E et Y une partie non vide de E, on définit la distance entre x et Y par

$$d(x, Y) = d(\{x\}, Y) = \inf\{d(x, y),\ y \in Y\}.$$

Théorème 1.8 – **Perpendiculaire commune à deux droites.**
Soit E un espace affine euclidien dont on note d la distance. Soient D et D' deux droites distinctes, non parallèles et non concourantes de E. Il existe un unique couple de points distincts $(M, M') \in D \times D'$ tel que (MM') soit orthogonale à D et à D'. De plus, on a $d(D, D') = ||\overrightarrow{MM'}||$.

Démonstration : Soient $A \in D$ et $A' \in D'$. Soient $\overrightarrow{u}$ et $\overrightarrow{u}'$ dans $\overrightarrow{E}$, de norme 1, tels que $\overrightarrow{D} = \mathbb{R}\overrightarrow{u}$ et $\overrightarrow{D'} = \mathbb{R}\overrightarrow{u}'$. A tout couple $(M, M') \in D \times D'$ ont peut associer un unique couple $(k, k') \in \mathbb{R}^2$ tel que $\overrightarrow{AM} = k\overrightarrow{u}$ et $\overrightarrow{A'M'} = k'\overrightarrow{u}'$.

On a alors $\overrightarrow{MM'} = \overrightarrow{MA} + \overrightarrow{AA'} + \overrightarrow{A'M'} = -k\overrightarrow{u} + \overrightarrow{AA'} + k'\overrightarrow{u}'$. Il s'ensuit que (MM') est orthogonale à D et D' si et seulement si $(\overrightarrow{u}|\overrightarrow{MM'}) = (\overrightarrow{u}'|\overrightarrow{MM'}) = 0$, c'est à dire si et seulement si le couple (k, k') associé à (M, M') vérifie le système

$$\begin{cases} k - k'(\overrightarrow{u}'|\overrightarrow{u}) &= (\overrightarrow{AA'}|\overrightarrow{u}) \\ k(\overrightarrow{u}'|\overrightarrow{u}) - k' &= (\overrightarrow{AA'}|\overrightarrow{u}') \end{cases}.$$

Le déterminant de ce système est $(\overrightarrow{u}|\overrightarrow{u}')^2 - 1$. Ce déterminant est donc nul si et seulement si $(\overrightarrow{u}|\overrightarrow{u}')^2 = ||\overrightarrow{u}||||\overrightarrow{u}'||$. Mais on sait (cas d'égalité dans l'inégalité de Cauchy-Schwarz) que ceci à lieu si et seulement si $\overrightarrow{u}$ et $\overrightarrow{u}'$ sont colinéaires, ce qui n'est pas le cas. Le système ci-dessus admet donc une solution et une seule. Ceci montre qu'il existe un unique couple de points distincts $(M, M') \in D \times D'$ tel que (MM') soit orthogonale à D et à D'. (Le fait que M et M' soient distincts est assuré puisque D et D' sont non concourantes.)

Enfin, pour $m \in D$ et $m' \in D'$, on a $\overrightarrow{mm'} = \overrightarrow{mM} + \overrightarrow{MM'} + \overrightarrow{M'm'}$, cette somme étant constituée de vecteurs deux-à-deux orthogonaux. Ainsi, $d(m, m')^2 = ||\overrightarrow{mm'}||^2 = ||\overrightarrow{mM}||^2 + ||\overrightarrow{MM'}||^2 + ||\overrightarrow{M'm'}||^2$. On a donc $d(m, m')^2 \geq d(M, M')^2$. Ceci montre que $d(M, M') = d(D, D')$. ∎

On a déjà défini, dans le cadre affine, les notions de projection, symétrie et affinité. On peut maintenant introduire celles de projection, symétrie et affinité orthogonales.

Définition 1.9 – *Soit E un espace affine euclidien et V un sous-espace affine de E.*
1. La projection orthogonale sur V est la projection affine de E sur V, parallèlement à $\overrightarrow{V}^{\perp}$.
2. La symétrie orthogonale par rapport à V est la symétrie affine de E par rapport à V, parallèlement à $\overrightarrow{V}^{\perp}$.
3. Soit $k \in \mathbb{R}$. L'affinité orthogonale par rapport à V et de rapport k est l'affinité affine de rapport k de E par rapport à V, parallèlement à $\overrightarrow{V}^{\perp}$.

Exercice 1.10 – Soit E un espace affine euclidien et V un sous-espace affine de E. Pour tout point m de E, la distance de m à V est $||\overrightarrow{mp(m)}||$, où p est la projection orthogonale sur V.

Exercice 1.11 – Soient E un espace affine euclidien de dimension $n \in \mathbb{N}^*$ et $R = (O, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ un repère cartésien orthonormé de E. On considère un hyperplan affine H de E dont l'équation dans R est $a_1x_1 + \ldots + a_nx_n + b = 0$.
1. Soit m un point de E dont on note $(m_1, \ldots, m_n)$ les coordonnées dans le repère R. Calculer les coordonnées de l'image $p(m)$ de m par la projection orthogonale p sur H.
2. Soit m un point de E dont on note $(m_1, \ldots, m_n)$ les coordonnées dans le repère R. Montrer que

$$d(m, H) = \left| \frac{b + \sum_{i=1}^n a_i m_i}{\sqrt{\sum_{i=1}^n a_i^2}} \right|.$$

2 Isométries affines.

On introduit maintenant la notion, très importante, d'isométrie.

Définition 2.1 – *Soient E et E' deux espaces affines euclidiens dont on note d et d' les distances respectives. Une isométrie de E dans E' est une application $f : E \longrightarrow E'$ telle que, pour tous $x, y \in E$, $d'(f(x), f(y)) = d(x, y)$.*

Remarque 2.2 – Soient E et E' deux espaces affines euclidiens (dont on note d et d' les distances respectives) et $f : E \longrightarrow E'$ une isométrie. Il est clair que f est nécessairement injective. Ainsi, f induit une bijection de E sur l'image de f.

Dans la suite, on va limiter notre étude au cas des isométries d'un espace affine euclidien E dans lui-même.

Définition 2.3 – *Soit E un espace affine euclidien. On note $Is(E)$ l'ensemble des isométries de E.*

Remarque 2.4 – Soit $\mathcal{E}$ un espace vectoriel euclidien dont on note $(-|-)$ le produit scalaire et $||-||$ la norme associée.
1. Alors, pour $x, y \in \mathcal{E}$, $2(x|y) = ||x+y||^2 - ||x||^2 - ||y||^2$.
2. On déduit du point 1 qu'une application linéaire de $\mathcal{E}$ est orthogonale si et seulement si elle conserve la norme.
3. On montre facilement que si une application $f : \mathcal{E} \longrightarrow \mathcal{E}$ conserve le produit scalaire (*i.e.*, pour tous $x, y \in \mathcal{E}$, $(f(x)|f(y)) = (x|y)$), alors elle est linéaire.

Lemme 2.5 – Soit E un espace affine et $f : E \longrightarrow E$ une isométrie. Alors, pour tout $a \in E$, f_a conserve le produit scalaire : pour tous $\overrightarrow{u}, \overrightarrow{v} \in \overrightarrow{E}$, on a $(f_a(\overrightarrow{u})|f_a(\overrightarrow{v})) = (\overrightarrow{u}|\overrightarrow{v})$.

Démonstration : Soient $\overrightarrow{u}, \overrightarrow{v} \in \overrightarrow{E}$. Il existe $x, y \in E$ tels que $\overrightarrow{u} = \overrightarrow{ax}$ et $\overrightarrow{v} = \overrightarrow{ay}$. On a alors :

$$\begin{aligned}
2(f_a(\overrightarrow{u})|f_a(\overrightarrow{v})) &= 2\left(\overrightarrow{f(a)f(x)}|\overrightarrow{f(a)f(y)}\right) \\
&= -2(\overrightarrow{f(x)f(a)}|\overrightarrow{f(a)f(y)}) \\
&= ||\overrightarrow{f(x)f(a)}||^2 + ||\overrightarrow{f(a)f(y)}||^2 - ||\overrightarrow{f(x)f(a)} + \overrightarrow{f(a)f(y)}||^2 \\
&= ||\overrightarrow{f(x)f(a)}||^2 + ||\overrightarrow{f(a)f(y)}||^2 - ||\overrightarrow{f(x)f(y)}||^2 \\
&= ||\overrightarrow{xa}||^2 + ||\overrightarrow{ay}||^2 - ||\overrightarrow{xy}||^2 \\
&= -2(\overrightarrow{xa}|\overrightarrow{ay}) \\
&= 2(\overrightarrow{ax}|\overrightarrow{ay}) \\
&= 2(\overrightarrow{u}|\overrightarrow{v})
\end{aligned}$$

.

Ceci montre l'assertion. ∎

Théorème 2.6 – *Soient E un espace affine euclidien et $f : E \longrightarrow E$ une application. Les assertions suivantes sont équivalentes :*
(i) f est une isométrie ;
(ii) f est une application affine et $\overrightarrow{f}$ est un automorphisme orthogonal de $\overrightarrow{E}$.

Démonstration : (ii) implique (i) est clair.
(i) implique (ii). On suppose donc que f est une isométrie. Soit $a \in E$ arbitraire et soit $f_a : \overrightarrow{E} \longrightarrow \overrightarrow{E}$ l'application définie par $f_a = \phi_{f(a)} \circ f \circ \phi_a^{-1}$ (c'est-à-dire par : pour tout $x \in E$,

$f_a(\overrightarrow{ax}) = \overrightarrow{f(a)f(x)}$). Le lemme 2.5 assure que f_a conserve le produit scalaire et la remarque 2.4 permet de conclure que f_a est linéaire. Il s'ensuit que f est affine. On a alors $\overrightarrow{f} = f_a$ qui conserve le produit scalaire, c'est-à-dire est orthogonal. ∎

Il découle du théorème 2.6 que $Is(E)$ est un sous-ensemble de $GA(E)$, et il est clair que c'est un sous-groupe de $GA(E)$. En fait, plus précisément, le théorème 2.6 assure que $Is(E) = \Theta_E^{-1}(O(E))$. Ainsi, le morphisme de groupe $\Theta_E : GL(A) \longrightarrow GL(E)$ induit un morphisme surjectif de groupes :

$$\theta_E : Is(E) \longrightarrow O(E).$$

Dans la suite, on note $Is^+(E)$ le sous-groupe de $Is(E)$ défini par $Is^+(E) = \theta_E^{-1}(O^+(E))$. Un élément de $Is^+(E)$ est appelé un déplacement de E. En outre, on note $Is^-(E)$ le sous-ensemble de $Is(E)$ défini par $Is^-(E) = \theta_E^{-1}(O^-(E))$. Un élément de $Is^-(E)$ est appelé un antidéplacement de E.

Le théorème suivant est très utile dans la pratique. Il permet, en particulier, de déterminer toutes les isométries du plan et de l'espace, comme on le verra plus loin. On commence par rappeler un résultat très important dans la suite.

Exercice 2.7 – Soient E un espace affine de direction $\overrightarrow{E}$ et $f : E \longrightarrow E$ une application affine. On note $\mathrm{Fix}(f)$ l'ensemble des points fixes de f : $\mathrm{Fix}(f) = \{m \in E \,|\, f(m) = m\}$.
1. Montrer que $\mathrm{Fix}(f)$ est soit vide soit un sous-espace affine de E de direction $\ker\left(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}\right)$.
2. On suppose E de dimension finie. Montrer que les assertions suivantes sont équivalentes :
(i) f admet un point fixe et un seul ;
(ii) $\ker\left(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}\right) = \{\overrightarrow{0}\}$.

Théorème 2.8 – *Soient E un espace affine euclidien et f une isométrie de E.*
1. On a $\overrightarrow{E} = \ker(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}) \oplus \mathrm{im}(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}})$.
2. Il existe un unique couple $(\overrightarrow{u}, g) \in \overrightarrow{E} \times Is(E)$ vérifiant les conditions suivantes :
(i) $\overrightarrow{u} \in \ker(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}})$;
(ii) g est un isométrie de E admettant un point fixe ;
(iii) $f = T_{\overrightarrow{u}} \circ g = g \circ T_{\overrightarrow{u}}$.

Démonstration : 1. Soit $\overrightarrow{u} \in \overrightarrow{E}$. Si $\overrightarrow{u} \in \ker(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}) \cap \mathrm{im}(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}})$, alors $\overrightarrow{f}(\overrightarrow{u}) = \overrightarrow{u}$ et il existe $\overrightarrow{v} \in \overrightarrow{E}$ tel que $\overrightarrow{u} = \overrightarrow{f}(\overrightarrow{v}) - \overrightarrow{v}$. On a alors $||\overrightarrow{u}||^2 = (\overrightarrow{u}|\overrightarrow{f}(\overrightarrow{v})) - (\overrightarrow{u}|\overrightarrow{v}) = (\overrightarrow{f}(\overrightarrow{u})|\overrightarrow{f}(\overrightarrow{v})) - (\overrightarrow{u}|\overrightarrow{v}) = 0$ car $\overrightarrow{f}$ est orthogonal.
2. Soit $a \in E$. D'après le premier point, il existe $\overrightarrow{u}$ et $\overrightarrow{v}$ dans $\overrightarrow{E}$ tels que $\overrightarrow{af(a)} = \overrightarrow{u} + (\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}})(\overrightarrow{v})$ et $\overrightarrow{f}(\overrightarrow{u}) = \overrightarrow{u}$. Posons $O = a - \overrightarrow{v}$, c'est-à-dire que O est le point de E tel que $\overrightarrow{v} = \overrightarrow{Oa}$. Alors, $\overrightarrow{f(O)O} = \overrightarrow{f(O)f(a)} + \overrightarrow{f(a)a} + \overrightarrow{aO} = (\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}})(\overrightarrow{Oa}) + \overrightarrow{f(a)a} = -\overrightarrow{u}$. Donc $f(O) = T_{\overrightarrow{u}}(O)$, ce qui montre que O est un point fixe de $T_{-\overrightarrow{u}} \circ f$. Il reste à poser $g = T_{-\overrightarrow{u}} \circ f$ pour obtenir la décomposition souhaitée.

Supposons maintenant que $(\overrightarrow{u}, g) \in \overrightarrow{E} \times Is(E)$ et $(\overrightarrow{u}', g') \in \overrightarrow{E} \times Is(E)$ vérifient les conditions de l'énoncé et notons O et O' les points fixes respectifs de g et g'. Alors, on a $\overrightarrow{u} = \overrightarrow{Of(O)}$ et $\overrightarrow{u}' = \overrightarrow{O'f(O')}$. Il s'ensuit que $\overrightarrow{f(O)f(O')} - \overrightarrow{OO'} = \overrightarrow{u}' - \overrightarrow{u} \in \ker(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}) \cap \mathrm{im}(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}) = \{\overrightarrow{0}\}$. Il s'ensuit que $\overrightarrow{u}' = \overrightarrow{u}$, puis que $g = g'$.

Montrons enfin que $T_{\overrightarrow{u}} \circ g = g \circ T_{\overrightarrow{u}}$. Comme ces applications affines ont même application linéaire associée, il suffit de montrer que l'image de O par l'une et par l'autre est la même. En

reprennant ce qui précède, on a que $\overrightarrow{Of(O)} = \overrightarrow{u} \in \ker(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}) = \ker(\overrightarrow{g} - \mathrm{id}_{\overrightarrow{E}})$ (cf. ex. 2.7), il s'ensuit que $f(O)$ est point fixe de g puisque O l'est. De ceci, on déduit facilement que $T_{\overrightarrow{u}} \circ g(O) = O + \overrightarrow{u} = f(O) = g \circ T_{\overrightarrow{u}}(O)$. ∎

On est maintenant en position de classer les isométries en dimension 2 et 3.

Isométries en dimension 2. Soient E un espace affine de dimension 2, $\overrightarrow{E}$ sa direction et $\{\overrightarrow{i}, \overrightarrow{j}\}$ une base orthonormale de référence à l'aide de laquelle on oriente $\overrightarrow{E}$. On considère une isométrie affine f de E dont on note $\overrightarrow{f}$ l'application linéaire associée.

1-ier cas : f est un déplacement. C'est-à-dire que $\overrightarrow{f} \in O^+(E)$.

1-ier sous-cas : $\overrightarrow{f} = \mathrm{id}_{\overrightarrow{E}}$. Il s'ensuit, d'après la proposition 3.7, que f est une translation.

2-ième sous-cas : $\overrightarrow{f} \neq \mathrm{id}_{\overrightarrow{E}}$. La classification des éléments du groupe orthogonal d'un espace euclidien de dimension 2 assure qu'il existe $\theta \in]0, 2\pi[$ tel que $\overrightarrow{f}$ soit la rotation de mesure d'angle θ. Ainsi, dans toute base orthonormale directe de $\overrightarrow{E}$, la matrice de $\overrightarrow{f}$ est

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

On sait qu'alors 1 n'est pas vecteur propre de $\overrightarrow{f}$. On en déduit, d'après l'exercice 2.7, que f admet un point fixe unique. Notons O ce point fixe. On dit que f est la rotation de centre O et de mesure d'angle θ.

2-ième cas : f est un antidéplacement. C'est-à-dire que $\overrightarrow{f} \in O^-(E)$.

On sait qu'alors, il existe une base orthonormale directe $\{\overrightarrow{e_1}, \overrightarrow{e_2}\}$ de $\overrightarrow{E}$ telle que la matrice de $\overrightarrow{f}$ dans cette base soit

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ainsi, $\overrightarrow{f}$ est la symétrie orthogonale par rapport à la droite vectorielle $\mathbb{R}\overrightarrow{e_1}$.

1-ier sous-cas : f a un point fixe. Soit O un point fixe de f. L'exercice 2.7 assure que $\mathrm{Fix}(f)$ est la droite D passant par O et de direction $\mathbb{R}\overrightarrow{e_1} = \ker(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}})$. Les théorèmes 4.5 et 4.6 assurent que f est la symétrie orthogonale de E par rapport à la droite D.

2-ième sous-cas : f n'a pas de points fixes. Le théorème de décomposition (théorème 2.8) assure qu'il existe un unique couple $(\overrightarrow{u}, g) \in \overrightarrow{E} \times Is(E)$ tel que $\overrightarrow{u} \in \ker(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}})$, g soit une isométrie de E admettant un point fixe et $f = T_{\overrightarrow{u}} \circ g = g \circ T_{\overrightarrow{u}}$.

Puisque g et f ont même partie linéaire, g est un antidéplacement qui possède un point fixe. Ainsi (cas précédent), g est la symétrie orthogonale par rapport à la droite $\mathrm{Fix}(g)$. Finalement, f est la composée d'une réflexion orthogonale par rapport à une droite D et d'une translation de vecteur $\overrightarrow{u}$ tel que $\overrightarrow{u} \in \overrightarrow{D} = \ker(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}})$.

En reprennant ce qui précède, on obtient facilement la table suivante permettant de déterminer la nature géométrique d'une isométrie d'un espace E de dimension 2 par la connaissance de

l'ensemble de ses points fixes.

Points fixes	Déplacement/antidépl.	Nature
plan	déplacement	identité
droite	antidéplacement	réflexion
point	déplacement	rotation
$\emptyset$	déplacement	translation
$\emptyset$	antidéplacement	symétrie glissée

Isométries en dimension 3. Soient E un espace affine de dimension 3, $\overrightarrow{E}$ sa direction et $\{\overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k}\}$ une base orthonormale de référence à l'aide de laquelle on oriente $\overrightarrow{E}$. On considère une isométrie affine f de E dont on note $\overrightarrow{f}$ l'application linéaire associée.

1-ier cas : f est un déplacement. C'est-à-dire que $\overrightarrow{f} \in O^+(E)$.

1-ier sous-cas : $\overrightarrow{f} = \mathrm{id}_{\overrightarrow{E}}$. Il s'ensuit, d'après la proposition 3.7, que f est une translation.

2-ième sous-cas : $\overrightarrow{f} \neq \mathrm{id}_{\overrightarrow{E}}$ et f admet un point fixe. La classification des applications orthogonales assure que $\ker\left(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}\right)$ est de dimension 1 et l'exercice 2.7 montre alors que $\mathrm{Fix}(f)$ est une droite de direction $\ker\left(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}\right)$. On sait aussi qu'une fois choisi un vecteur $\overrightarrow{u} \in \ker\left(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}\right)$, il existe un unique réel $\theta \in]0, 2\pi[$ tel que la matrice de $\overrightarrow{f}$ dans toute base orthonormée directe commençant par $\overrightarrow{u}$ soit

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

On dit alors que f est la rotation affine d'axe $\mathrm{Fix}(f)$ (orienté par $\overrightarrow{u}$) et de mesure d'angle θ (relativement au choix de $\overrightarrow{u}$).

3-ième sous-cas : $\overrightarrow{f} \neq \mathrm{id}_{\overrightarrow{E}}$ et f n'admet pas de point fixe. Dans ce cas encore, $\ker\left(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}\right)$ est de dimension 1. Le théorème 2.8 assure alors qu'il existe $\overrightarrow{u} \in \ker\left(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}\right)$, non nul, et un déplacement g admettant un point fixe tel que $f = g \circ T_{\overrightarrow{u}} = T_{\overrightarrow{u}} \circ g$. L'étude du cas précédant montre que g est une rotation affine d'axe $\mathrm{Fix}(g)$ (orienté par $\overrightarrow{u}$) et de mesure d'angle θ (relativement au choix de $\overrightarrow{u}$). On dit alors que f est le vissage d'axe $\mathrm{Fix}(g)$ (orienté par $\overrightarrow{u}$) et de mesure d'angle θ (relativement au choix de $\overrightarrow{u}$) et de vecteur $\overrightarrow{u}$.

2-ième cas : f est un antidéplacement. C'est-à-dire que $\overrightarrow{f} \in O^-(E)$.

La classification des applications orthogonales assure que $\ker\left(\overrightarrow{f} + \mathrm{id}_{\overrightarrow{E}}\right)$ est de dimension au moins 1 et qu'une fois choisi un vecteur $\overrightarrow{u} \in \ker\left(\overrightarrow{f} + \mathrm{id}_{\overrightarrow{E}}\right)$, il existe un unique réel $\theta \in [0, 2\pi[$ tel que la matrice de $\overrightarrow{f}$ dans toute base orthonormée directe commençant par $\overrightarrow{u}$ soit

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

1-ier sous-cas : $\overrightarrow{f}$ admet 1 pour valeur propre (*i.e.* $\theta = 0$).
a) Si f a un point fixe, alors $\mathrm{Fix}(f)$ est un espace affine de dimension 2 et f est le symétrie orthogonale par rapport au plan $\mathrm{Fix}(f)$.
b) Si f n'a pas de points fixes, en utilisant le théorème de décomposition, on se ramène au cas a) et on montre que f est une *symétrie glissée*, c'est-à-dire la composée d'une symétrie orthogonale par rapport au plan $\mathrm{Fix}(g)$ de direction $\ker\left(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}\right)$ et d'une translation de vecteur $\overrightarrow{u} \in \ker\left(\overrightarrow{f} - \mathrm{id}_{\overrightarrow{E}}\right)$.

2-ième sous-cas : $\overrightarrow{f}$ n'admet pas 1 pour valeur propre (*i.e.* $\theta \neq 0$). Dans ce cas, f admet un point fixe unique et on dit que f est une antirotation affine. On montre facillement que f est le produit (commutatif) d'une rotation affine et d'une symétrie orthogonale par rapport à un plan orthogonal à l'axe de rotation.

En reprennant ce qui précède, on obtient facilement la table suivante permettant de déterminer la nature géométrique d'une isométrie d'un espace E de dimension 3 par la connaissance de l'ensemble de ses points fixes.

Points fixes	Déplacement/antidépl.	Nature
espace	déplacement	identité
plan	antidéplacement	réflexion
droite	déplacement	rotation
point	antidéplacement	antirotation
$\emptyset$	déplacement	translation
$\emptyset$	antidéplacement	symétrie glissée
$\emptyset$	déplacement	vissage

3 *Exercices.*

§A - *Problèmes de base.*

Exercice 3.1 – Hyperplan médiateur.
Soit E un espace affine euclidien. On considère deux points A et B distincts de E.
1. Montrer qu'il existe une et une seule réflexion de E qui échange A et B. L'hyperplan associé à cette réflexion est appelé l'hyperplan médiateur de A et B (ou de $[AB]$).
2. Montrer que l'hyperplan médiateur de A et B est l'ensemble des points équidistants de A et de B.

Exercice 3.2 – Convexité.
Soit E un espace affine. Une partie X de E est dite convexe si elle est non vide et si, pour tous $A, B \in X$, on a $[A, B] \subseteq X$.
1. Soit E un espace affine
1.1. Montrer que tout segment de E est une partie convexe.
Indication. On pourra commencer par remarquer que, si $A, B \in E$, $[A, B]$ est l'ensemble des points M de E pour lesquels il existe $\lambda \in [0, 1]$ tel que $\overrightarrow{AM} = \lambda\overrightarrow{AB}$.
1.2. Soit F un sous-espace affine de E. Montrer que F est une partie convexe de E.
1.3. Soit A un point de E et $\overrightarrow{u}$ un élément de $\overrightarrow{E}$. On appelle demi-droite fermée (resp. ouverte) d'origine A et de vecteur directeur $\overrightarrow{u}$ l'ensemble des points M de E pour lesquels il existe $\lambda \in \mathbb{R}_+$

(resp. $\lambda \in \mathbb{R}_+^*$) tel que $\overrightarrow{AM} = \lambda \overrightarrow{u}$. Montrer qu'une demi-droite ouverte ou fermée est une partie convexe de E.
2. Soient E un espace affine et I un ensemble non vide. Montrer que l'intersection d'une famille de parties convexes de E indexée par I est soit vide soit une partie convexe de E.
3. Soient E et F des espaces affines et $f : E \longrightarrow F$ une application affine. Montrer que l'image d'une partie convexe de E est une partie convexe de F. Montrer que l'image réciproque d'une partie convexe de F est soit vide soit une partie convexe de E.

Exercice 3.3 – Soit E un espace affine de dimension n, $n \in \mathbb{N}^*$. On considère un hyperplan affine H de E.
1. On définit la relation binaire $\mathcal{R}$ sur $E \setminus H$ de la façon suivante. Soient A et B deux points de $E \setminus H$, on note $A\mathcal{R}B$ si $[A, B] \cap H = \emptyset$. Le but de cette question est de montrer que $\mathcal{R}$ est une relation d'équivalence. Si deux points sont en relation par $\mathcal{R}$, on dit que *A et B sont du même coté de H*.
1.1. Soit R un repère de E. L'application $\iota : E \longrightarrow \mathbb{R}^n$ qui à un point de E associe le n-uplet de ses coordonnées dans R est un isomorphisme d'espaces affines. On considère $\alpha_0, \ldots, \alpha_n \in \mathbb{R}$ tels qu'une équation de H dans R soit $\alpha_0 + \sum_{i=1} \alpha_i x^i = 0$. Ainsi, $\iota(H)$ est le noyau de l'application affine $f : \mathbb{R}^n \longrightarrow \mathbb{R}$, $(x_1, \ldots, x_n) \mapsto \alpha_0 + \sum_{i=1} \alpha_i x^i$.

Soient A et B des points de $E \setminus H$. Montrer que $A\mathcal{R}B$ si et seulement si $f \circ \iota(A) f \circ \iota(B) > 0$ (autrement dit, $f \circ \iota(A)$ et $f \circ \iota(B)$ ont même signe).
1.2. Conclure.
Les deux classes d'équivalences définies par cette relation d'équivalence s'appelent les demi-espaces ouverts associés à H. Les demi-espaces fermés associés à H sont les réunions de chaque demi-espace ouvert avec H.
2. On suppose E muni d'une structure euclidienne (et donc d'une structure d'espace métrique).
2.1. Montrer que les demi-espaces ouverts définis par H sont des ouverts de l'espace métrique E. Montrer que les demi-espaces fermés définis par H sont des fermés de l'espace métrique E.
2.2. Montrer que les demi-espaces (ouverts ou fermés) définis par H sont des parties convexes de E.

§B - *Engendrement des groupes d'isométries (dim. 2 et 3).*

Exercice 3.4 – **Réflexions dans le plan affine.**
Soit E un espace affine euclidien orienté de dimension 2.
1. Composée de réflexions. On considère deux droites D et D' de E et on note, respectivement, s et s' les réflexions par rapport à D et D'.
1.1. Décrire $s' \circ s$ lorsque D et D' sont parallèles.
1.2. Décrire $s' \circ s$ lorsque D et D' ne sont pas parallèles.
2. Montrer que le groupe $Is(E)$ est engendré par les réflexions.

Exercice 3.5 – **Réflexions dans l'espace affine de dimension 3.**
Soit E un espace affine euclidien orienté de dimension 3.
1. Composée de réflexions. On considère deux plans P et P' de E et on note, respectivement, s et s' les réflexions par rapport à P et P'.
1.1. Décrire $s' \circ s$ lorsque P et P' sont parallèles.
1.2. Décrire $s' \circ s$ lorsque P et P' ne sont pas parallèles.
2. Montrer que le groupe $Is(E)$ est engendré par les réflexions.

Exercice 3.6 – **Demi-tours.**
Soit E un espace affine euclidien de dimension 3. On appelle demi-tour de E toute symétrie orthogonale par rapport à une droite. Le but de cet exercice est de montrer que l'ensemble des demi-tours engendre $Is^+(E)$.
1. Soient D et D' deux droites de E. Soient s et s' les demi-tours par rapport à D et D', respectivement.
1.1. Montrer que, si D et D' sont parallèles, alors $s' \circ s$ est une translation et décrire cette translation.
1.2. Montrer que, si D et D' sont sécantes, alors $s' \circ s$ est une rotation et décrire cette rotation.
1.3. Montrer que, si D et D' ne sont ni sécantes ni parallèles, alors $s' \circ s$ est un vissage et décrire ce vissage.
2. Conclure.

§C - *Etudes pratiques d'isométries (dim. 2 et 3).*

Exercice 3.7 – Soient E un espace affine euclidien de dimension 3 et $R = (O, \overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k})$ un repère cartésien orthonormé direct de E. On considère les points suivants, donnés par leurs coordonnées dans R : $A(1,1,1)$, $B(-1,1,1)$, $C(-1,-1,1)$, $D(1,-1,1)$, $A'(1,1,-1)$, $B'(-1,1,-1)$, $C'(-1,-1,-1)$, $D'(1,-1,-1)$ (ce sont les sommets d'un cube centé en O et de longueur d'arête 2). En outre, on considère les isométries suivantes :
- σ_1 : symétrie orthogonale par rapport à la droite (AC) ;
- σ_2 : symétrie orthogonale par rapport à la droite (BD') ;
- σ_3 : symétrie orthogonale par rapport au plan (ABC).
1. Ecrire l'expression analytique de σ_1, σ_2 et σ_3 dans R.
2. Préciser la nature géométrique de $\sigma_1 \circ \sigma_2$.
3. Préciser la nature géométrique de $\sigma_2 \circ \sigma_3$.

Exercice 3.8 – Soient E un espace affine euclidien de dimension 3 et $R = (O, \overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k})$ un repère cartésien orthonormé direct de E. On considère les droites D_1 et D_2 de E dont les représentations cartésiennes dans R sont, respectivement :

$$\begin{cases} x+y+z=1 \\ x+2y+z=2 \end{cases} \quad \text{et} \quad \begin{cases} x=1 \\ x+2y+z=-2 \end{cases}$$

1. Donner une représentation paramétrique de D_1 et D_2 dans R.
2. Décrire l'image d'un point de coordonnée (x,y,z) dans R par la symétrie orthogonale S_1 par rapport à D_1 et par la symétrie orthogonale S_2 par rapport à D_2.
3. On considère l'isométrie $u = S_1 \circ S_2$. Montrer que u est un déplacement sans points fixes, admettant une droite Δ globalement invariante. En déduire que u est un vissage et le décrire géométriquement.
4. Décrire $S_2 \circ S_1$.

§D - *Sous-groupes d'isométries laissant invariant un ensemble.*

Exercice 3.9 – **Le groupe diédral.**
On se place dans l'espace affine euclidien E de dimension 2, muni d'un repère orthonormé $R = (O, \overrightarrow{i}, \overrightarrow{j})$ avec lequel on oriente E. On considère le point A_0 de E de coordonnées $(1,0)$ dans R. On note n un entier supérieur ou égal à 3 et r la rotation de centre O et de mesure d'angle $2\pi/n$. Pour $i \in \mathbb{Z}$, on pose $A_i = r^i(A_0)$ et $\mathcal{S}_n = \{A_i,\, i \in \mathbb{Z}\}$.

1. Montrer que $\mathcal{S}_n = \{A_0, \ldots, A_{n-1}\}$.
2. Montrer que O est l'isobarycentre de $\mathcal{S}_n$.
3. On note D_n l'ensemble des isométries f de E telles que $f(\mathcal{S}_n) = \mathcal{S}_n$.
3.1. Montrer que D_n est un sous-groupe de $Is^+(E)$. On l'appelle le groupe diédral d'ordre n.
3.2. Montrer que tout élément de D_n admet O pour point fixe.
3.3. Déterminer tous les éléments de $D_n \cap Is^+(E)$.
3.4. On note s la réflexion par rapport à la droite (OA_0). Montrer que $s \in D_n$.
3.5. Montrer que la composition à droite par s définit une application bijective $D_n \cap Is^+(E) \longrightarrow D_n \cap Is^-(E)$. En déduire que D_n est d'ordre $2n$ et que $D_n = \{\mathrm{id}_E, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$.
3.6. Montrer que $sr = r^{n-1}s$. En déduire la table de multiplication de D_n.
3.7. Décrire géométriquement les éléments de D_n.

§E - *Similitudes affines.*

Exercice 3.10 – Soit E un espace affine euclidien dont on note d la distance. Si $k \in \mathbb{R}_+^*$, on appelle similitude de rapport k toute application $f : E \longrightarrow E$ telle que, pour tous $x, y \in E$, $d(f(x), f(y)) = d(x, y)$.
1. Montrer l'équivalence des assertions suivantes :
(i) f est une similitude ;
(ii) f est affine et $\overrightarrow{f}$ est une similitude vectorielle ;
(iii) f est la composée d'une homothétie de rapport non nul et d'une isométrie.
2. Soit f une similitude de rapport $k \in \mathbb{R}_+^*$, avec $k \neq 1$. Montrer que f admet un point fixe unique Ω. On note h l'homothétie de centre Ω et de rapport k. Montrer que $g = h^{-1} \circ f$ est une isométrie de E dont Ω est un point fixe. Montrer que $f = h \circ g = g \circ h$.
Note. L'unique point invariant d'une similitude de rapport k différent de 1 est appelé son centre.
3. Soit $f : E \longrightarrow E$ une application affine non constante. Montrer que les assertions suivantes sont équivalentes :
(i) f est une similitude ;
(ii) f conserve l'orthogonalité (*i.e.* si A, B, C sont des points de E tels que $(\overrightarrow{AB}|\overrightarrow{AC}) = 0$, alors $(\overrightarrow{f(A)f(B)}|\overrightarrow{f(A)f(C)}) = 0$.

§F - *Coniques.*

Exercice 3.11 – **Equation de coniques ; réduction.**
On se place dans le plan affine euclidien.
1. Soit C un ensemble de points de E. Montrer que les assertions suivantes sont équivalentes :
(i) il existe un repère R de E tel que les points de C sont ceux dont les coordonnées dans R vérifient une équation polynômiale en deux indéterminées et de degré 2 ;
(ii) dans tout repère R de E, les points de C sont ceux dont les coordonnées dans R vérifient une équation polynômiale en deux indéterminées et de degré 2.
Un ensemble de points de E vérifiant ces assertions s'appelle une conique généralisée de E.
2. Soit R un repère orthonormé de E. On considère une conique généralisée E et des réels a, b, c, d, e, f tels que $(a, b, c) \neq (0, 0, 0)$ pour lesquels C est l'ensemble des points de E dont les coordonnées dans R vérifient l'équation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0. \qquad (*)$$

On dit que $(*)$ est l'équation de C dans R.
2.1. Montrer qu'il existe un repère orthonormé de E et des réels A, C, D, E, F tels que l'équation

de C dans ce repère soit

$$Ax^2 + Cy^2 + Dx + Ey + F = 0. \qquad (**)$$

2.2. On reprend les notations de 2.1 et on suppose $A \neq 0$ et $C \neq 0$. Montrer qu'il existe un repère orthonormé de E et des réels α, β, γ tels que l'équation de C dans ce repère soit

$$\alpha x^2 + \beta y^2 + \gamma = 0.$$

Décrire C.
2.3. On reprend les notations de 2.1 et on suppose $A \neq 0$ et $C = 0$. Montrer qu'il existe un repère orthonormé de E et des réels α, β, γ tels que l'équation de C dans ce repère soit

$$\alpha x^2 + \beta y + \gamma = 0.$$

Décrire C.
3. On se place dans l'espace affine euclidien et on le rapporte à son repère orthonormal canonique. Dans chacun des cas suivants, décrire la conique généralisée dont l'équation dans R est donnée :
3.1. $3x^2 + 2xy - y^2 - 10x + 6y - 8 = 0$;
3.2. $x^2 + 2xy + y^2 - 2x + 2y = 0$;
3.3. $xy + 3x + 2y - 6 = 0$;
3.4. $2mx^2 - 8mx - (m-1)y^2 + 12m - 2 = 0$, où m est un paramètre réel ;
3.5. $x^2 + y^2 + 4xy - 6x + 6y + 9 = 0$.

Exercice 3.12 – **Paramétrisation des coniques.**
On se place dans le plan affine euclidien rapporté à un repère orthonormé $R = (O, \overrightarrow{i}, \overrightarrow{j})$.
1. Soit $p \in \mathbb{R}_+^*$. On considère la parabole P de E de foyer F de coordonnées $(p/2, 0)$ et de directrice D d'équation $x = -p/2$ dans R. L'équation de P dans R est donc $y^2 = 2px$.
1.1. Montrer que P admet

$$\begin{cases} x = \dfrac{t^2}{2p} \ (t \in \mathbb{R}) \\ y = t \end{cases}$$

pour représentation paramétrique dans R.
1.2. Déterminer une équation cartésienne de la tangente à P en un point M de coordonnées (x, y).
1.3. Montrer que la tangente à P en un point M de P est la hauteur issue de M du triangle (MFH), où H est le projeté orthogonal de M sur D.
2. On considère deux nombres réels a, b tels que $0 < b \leq a$ et on pose $c = \sqrt{a^2 - b^2}$. On considère l'ellipse E de foyer F de coordonnées $(c, 0)$, de directrice d'équation $x = a^2/c$ et d'excentricité c/a. L'équation de E dans R est donc

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

2.1. Montrer que E admet

$$\begin{cases} x = a\cos(t) \\ y = b\sin(t) \end{cases} \ (t \in [0, 2\pi[)$$

pour représentation paramétrique dans R.
2.2. Déterminer une équation cartésienne de la tangente à E en un point M de coordonnées (x, y).

2.3. Montrer que la tangente à E en un point M est dirigée par un vecteur orthogonal à $\frac{\overrightarrow{MF}}{||\overrightarrow{MF}||} + \frac{\overrightarrow{MF'}}{||\overrightarrow{MF'}||}$, où F' est le second foyer de E.

3. On considère deux nombres réels a, b tels que $0 < b, a$ et on pose $c = \sqrt{a^2 + b^2}$. On considère l'hyperbole H de foyer F de coordonnées $(c, 0)$, de directrice d'équation $x = a^2/c$ et d'excentricité c/a. L'équation de E dans R est donc

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1.$$

3.1. Montrer que E admet

$$\begin{cases} x = \pm a\cosh(t) \\ y = b\sinh(t) \end{cases} (t \in \mathbb{R})$$

pour représentation paramétrique dans R.

3.2. Déterminer une équation cartésienne de la tangente à E en un point M de coordonnées (x, y).

3.3. Montrer que la tangente à E en un point M est dirigée par $\frac{\overrightarrow{MF}}{||\overrightarrow{MF}||} + \frac{\overrightarrow{MF'}}{||\overrightarrow{MF'}||}$, où F' est le second foyer de E.

Exercice 3.13 – On se place dans le plan affine euclidien. Soit E une ellipse de foyer F et de directrice D. Soit M un point de E distinct des sommets de l'ellipse et T_M la tangente à E en M. On note H le point d'intersection de T_M et D. Montrer que les vecteurs $\overrightarrow{FM}$ et $\overrightarrow{FH}$ sont orthogonaux.

Exercice 3.14 – On se place dans le plan affine euclidien. Soit H une hyperbole de foyer F et de directrice D. On note C le cercle de diamètre $[AA']$, où A et A' sont les sommets de l'hyperbole. Montrer que l'ensemble des projections orthogonale de F sur les tangentes à H est $C \setminus (C \cap D)$.

§G - *Problèmes d'angles.*

Exercice 3.15 – **Somme des angles d'un triangle.** Soit E un espace affine euclidien de dimension 2, orienté. On considère trois points A, B, C non alignés de E (c'est-à-dire un triangle non applati). Montrer que la somme des (mesures des) angles définis par ce triangle est égale à π modulo 2π, c'est-à-dire que :

$$\text{mes}(\widehat{\overrightarrow{AB}, \overrightarrow{AC}}) + \text{mes}(\widehat{\overrightarrow{CA}, \overrightarrow{CB}}) + \text{mes}(\widehat{\overrightarrow{BC}, \overrightarrow{BA}}) = \pi + 2\pi\mathbb{Z}.$$

Exercice 3.16 – **Le théorème de l'angle inscrit.** Soit E un espace affine euclidien de dimension 2, orienté. On considère un cercle ω de centre O et deux points A et B de ω. On note T_A la tangente à ω en A,

1. Montrer que, si M est un point de ω distinct de A et de B, alors :

$$\text{mes}(\widehat{\overrightarrow{OA}, \overrightarrow{OB}}) = 2\text{mes}(\widehat{\overrightarrow{MA}, \overrightarrow{MB}}).$$

2. Montrer que, si M est un point de ω distinct de A et de B, alors :

$$\text{mes}(\widehat{T_A, (AB)}) = \text{mes}(\widehat{(MA), (MB)}).$$

Exercice 3.17 – Cocyclicité.
Soit E un espace affine de dimension 2 muni d'un repère orthonormé avec lequel on l'oriente. On considère deux points A, B distincts de E et un réel a. On pose

$$E_\pi(A,B,a) = \{M \in E \setminus \{A,B\} \,|\, \text{mes}(\widehat{\overrightarrow{MA}, \overrightarrow{MB}}) = a(\text{mod } \pi)\}.$$

1. On suppose $a = 0(\text{mod } \pi)$. Montrer que $E_\pi(A,B,a) = (AB) \setminus \{A,B\}$.
2. On suppose $a \neq 0(\text{mod } \pi)$. On note ω le cercle contenant A et B et dont la tangente, T_A, en A vérifie $\text{mes}(\widehat{T_A, (AB)}) = a(\text{mod } \pi)$. Montrer que, si $a \neq 0(\text{mod } \pi)$, alors $E_\pi(A,B,a) = \omega \setminus \{A,B\}$.
3. Soient A, B, C, D quatre points distincts de E. Montrer que A, B, C, D sont alignés ou cocycliques si et seulement si $\text{mes}(\widehat{\overrightarrow{CA}, \overrightarrow{CB}}) = \text{mes}(\widehat{\overrightarrow{DA}, \overrightarrow{DB}})(\text{mod } \pi)$.

Exercice 3.18 – Arc capable.
Soit E un espace affine de dimension 2 muni d'un repère orthonormé avec lequel on l'oriente. On considère deux points A, B distincts de E et un réel a. On pose

$$E_{2\pi}(A,B,a) = \{M \in E \setminus \{A,B\} \,|\, \text{mes}(\widehat{\overrightarrow{MA}, \overrightarrow{MB}}) = a(\text{mod } 2\pi)\}.$$

1. On suppose $a = 0(\text{mod } 2\pi)$. Montrer que $E_{2\pi}(A,B,a) = (AB) \setminus [A,B]$.
2. On suppose $a = \pi(\text{mod } 2\pi)$. Montrer que $E_{2\pi}(A,B,a) =]A,B[$.
3. On suppose $a \neq 0(\text{mod } \pi)$. On note T un point de E distinct de A et tel que $\text{mes}(\widehat{\overrightarrow{AT}, \overrightarrow{AB}}) = a(\text{mod } 2\pi)$ et ω le cercle passant pas A et B et dont la tangente en A est la droite (AT). Montrer que $E_{2\pi}(A,B,a)$ est l'intersection du cercle ω et du demi-plan ouvert déterminé par (AB) ne contenant pas T.

Indication. Pour la troisième question, on pourra utiliser les exercices 6.31 et 3.17.

Partie X

Appendice : lexique sur les structures fondamentales.

1 *La notion de groupe.*

Rappelons qu'étant donné un ensemble E, une loi de composition interne (l.c.i.) de E est une application de $E \times E$ dans E qui à tout couple (a, b) d'éléments de E associe un troisième élément de E. Dans le contexte qui nous intéresse, cet élément est souvent – mais pas exclusivement – noté ab (c'est la notation dite multiplicative).

La première structure algébrique importante est celle de groupe. Un groupe est un ensemble muni d'une seule loi de composition interne. Dans les exemples intéressants dans la pratique, cette loi est parfois commutative mais beaucoup de groupes non commutatifs nous seront utiles.

1.1 Définitions fondamentales.

Définition 1.1.1 – *Un groupe est un ensemble G muni d'une loi de composition interne $G \times G \longrightarrow G : (a, b) \mapsto ab$ qui vérifie les propriétés suivantes :*
1. $(ab)c = a(bc)$ pour $a, b, c \in G$ (associativité),
2. il existe $e \in G$ tel que $ae = ea = a$ pour tout $a \in G$ (e est appelé neutre),
3. pour tout $a \in G$, il existe $a' \in G$ tel que $aa' = a'a = e$ (a' est appelé inverse de a).

Exemple 1.1.2 – Les exemples de groupes sont très nombreux et très variés.
1. L'ensemble $\mathbb{Z}$ des entiers relatifs muni de son addition est un groupe.
2. Si $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, l'ensemble $\mathbb{K}$ muni de la loi de composition interne d'addition $\mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{K} : (a, b) \mapsto a + b$ est un groupe (noter qu'ici, la notation multiplicative est à proscrire car elle a une autre signification).
3. Si $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, l'ensemble $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ muni de la loi de composition interne de multiplication (au sens usuel) $\mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{K} : (a, b) \mapsto ab$ est un groupe (ici, la notation multiplicative s'impose).
4. Étant donné un ensemble E, on note $\mathrm{Sym}(E)$ l'ensemble des bijections de E dans E. On muni $\mathrm{Sym}(E)$ de la loi de composition des applications. On obtient ainsi un groupe appelé le groupe symétrique de E. En effet, la loi de composition des applications est associative (comme on l'a déjà remarqué plus haut), l'application identité id_E (qui envoie un élément de E sur lui-même) est un élément neutre et, si f est une bijection de E dans E, elle admet une bijection réciproque g qui est inverse de f puisque $f \circ g = g \circ f = \mathrm{id}_E$.

Remarque 1.1.3 – **Un point de notation.** On est parfois amené à utiliser, pour désigner un groupe, une notation condensée faisant apparaître explicitement sa loi de composition interne. Ainsi, si l'on reprend les exemples 1.1.2, $\mathbb{Z}$ est un groupe pour l'addition et on parle du groupe $(\mathbb{Z}, +)$. De même, si $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, $\mathbb{K}$ est un groupe pour l'addition, que l'on note $(\mathbb{K}, +)$ et $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ est un groupe pour la multiplication, que l'on note $(\mathbb{K}^*, \times)$. Enfin, pour un ensemble E, $\mathrm{Sym}(E)$ muni de la composition des applications est noté $(\mathrm{Sym}(E), \circ)$.

Remarque 1.1.4 – Réexaminons la définition 1.1.1.
1. L'axiome d'associativité signifie que, si l'on veut multiplier trois élément a, b, c de G, l'ordre dans lequel on procède n'a pas d'importance. Ainsi, au lieu d'écrire $a(bc)$ (qui signifie qu'on multiplie d'abord b et c puis a et bc) ou $(ab)c$ (qui signifie qu'on multiplie d'abord a et b puis ab et c) on peut se contenter d'écrire abc sans autre précision. Cette remarque s'étend au produit d'un nombre quelconque d'éléments de G.
2. Dans un groupe G, il existe un seul élément neutre. Soient en effet e et e' deux éléments neutres de G. Comme e est neutre, on doit avoir $ee' = e'e = e'$. Comme e' est neutre, on doit

avoir $ee' = e'e = e$. Il s'ensuit que $e = e'$. On peut donc parler de l'élément neutre de G.
3. Pour tout élément a d'un groupe G, il existe un seul inverse. Soient en effet a' et a'' deux inverses de a. Comme a' est inverse de a, on doit avoir $aa' = a'a = e$. Comme a'' est inverse de a, on doit avoir $aa'' = a''a = e$. On a donc $a'a = a''a$ et si l'on multiplie cette identité à droite par a', on obtient $a' = a''$. On peut donc parler de l'inverse de a ; dans la notation multiplicative, il est noté a^{-1}.
4. Du fait de l'existence d'un inverse pour tout élément, on dispose des règles de simplification suivantes. Soient a, b, c dans G ; si $ab = ac$, alors $b = c$. C'est la règle de simplification à gauche. De même, on dispose d'une règle de simplification à droite. La démonstration de ces règles est laissée au lecteur en guise d'exercice facile.
5. Si a et b sont des éléments de G, alors l'inverse de ab est $b^{-1}a^{-1}$ (attention à l'ordre des facteurs). Cette propriété s'étend ainsi : si $a_1, \ldots, a_n$ sont n éléments de G, alors l'inverse de $a_1 \ldots a_n$ est $(a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}$. Là encore, la démonstration est laissée au lecteur.

Définition 1.1.5 – *Soit G un groupe (noté multiplicativement). Si $a, b \in G$ sont deux éléments tels que $ab = ba$, on dit que a et b commutent. Si a est un élément de G qui commute avec tout élément b de G, on dit que a est un élément central de G. L'ensemble des éléments centraux de G est appelé le centre de G et est noté $Z(G)$. Si $G = Z(G)$ (c'est-à-dire si $ab = ba$ pour tout couple (a, b) d'éléments de G) on dit que G est un groupe commutatif ou abélien.*

Exemple 1.1.6 – On reprend à nouveau les exemples 1.1.2. Il est clair que $(\mathbb{Z}, +)$, $(\mathbb{K}, +)$ et $(\mathbb{K}^*, \times)$ sont des groupes commutatifs. En revanche, pour un ensemble E, $(\mathrm{Sym}(E), \circ)$ n'est commutatif que si l'ensemble E contient au plus deux éléments. La démonstration de ce résultat est laissée en exercice.

Pour toute structure algébrique, il est indispensable d'introduire une notion de sous-structure. Il s'agit de distinguer, parmi les sous-ensembles de l'ensemble sous-jacent, ceux qui *respectent* (on dit aussi *se comportent bien vis-à-vis de*) la structure en question. L'importance cruciale de ces sous-structures apparait assez naturelle. Néanmoins elle sera mise en évidence de façon encore plus éclatante lorqu'il sera question des morphismes relatifs à la dite structure.

Définition 1.1.7 – *Soit G un groupe (noté multiplicativement) et H un sous-ensemble de G. On dit que H est un sous-groupe de G si les trois propriétés suivantes sont satisfaites.*
1. Pour $a, b \in H$, $ab \in H$ (on dit que H est stable sous la loi de composition interne de G) ;
2. $e \in H$ (c.à.d. que le neutre de G est un élément de H) ;
3. pour tout élément a de H, $a^{-1} \in H$ (c.à.d. que l'inverse a^{-1} de a dans G est dans H).

Remarque 1.1.8 – Si un sous-ensemble H d'un groupe G est un sous-groupe de G, alors la loi de composition interne $G \times G \longrightarrow G$ de G induit par restriction une loi de composition interne $H \times H \longrightarrow H$ et, muni de cette loi de composition interne, H est un groupe. C'est clair : le seul axiome nécessaire pour que H soit un groupe et qui n'est pas inclus dans la définition même de sous-groupe est l'associativité, mais l'associativité de la loi de composition interne de G garantit *a fortiori* celle de H (qui n'en est que la restriction).

Exemple 1.1.9 – Soit G un groupe dont l'élément neutre est noté e ; $\{e\}$ et G sont des sous-groupes de G.

Proposition 1.1.10 – *Soit G un groupe (noté multiplicativement), I un ensemble non vide et $(H_i)_{i \in I}$ une famille de sous-groupes de G. Alors $\cap_{i \in I} H_i$ est un sous-groupe de G.*

Démonstration : Exercice. ∎

À présent que l'on a introduit la notion de groupe, il semble naturel de disposer d'un moyen de comparer deux groupes. La notion appropriée pour atteindre ce but est celle de *morphisme de groupes.*

Définition 1.1.11 – *Soient G et G' deux groupes (notés multiplicativement). Un application $\phi : G \longrightarrow G'$ de G dans G' est un morphisme de groupe si, pour tous $g, h \in G$, on a $\phi(gh) = \phi(g)\phi(h)$. Si de plus ϕ est une bijection, alors on dit que ϕ est un isomorphisme de groupes.*

Exemple 1.1.12 –
1. L'application $\exp : \mathbb{C} \longrightarrow \mathbb{C}^*$ défini par $z \mapsto e^z$ est un morphisme surjectif et non injectif du groupe $\mathbb{C}$ muni de la loi d'addition des complexes dans le groupe $\mathbb{C}^*$ muni de la loi de multiplication des complexes.
2. L'application $|-| : \mathbb{C}^* \longrightarrow \mathbb{R}_+^*$ défini par $z \mapsto |z|$ est un morphisme surjectif et non injectif du groupe $\mathbb{C}^*$ muni de la loi de multiplication des complexes dans le groupe $\mathbb{R}_+^*$ muni de la loi de multiplication des réels.
3. Soit G un groupe (noté multiplicativement) et x un élément quelconque de G. Rappelons que, si $x \in G$ et $m \in \mathbb{N}^*$, on pose $x^m = x \dots x$ (m fois). On peut étendre cette notation pour $m \in \mathbb{Z}^*$: pour ce faire, si $m \in \mathbb{N}^*$, on pose $x^{-m} = (x^{-1})^m = x^{-1} \dots x^{-1}$ (m fois). Par convention, on pose $x^0 = e$, où e est le neutre de G. Il est clair alors que, si $m, m' \in \mathbb{Z}$ et $x \in G$, $x^m x^{m'} = x^{m+m'}$. Ainsi, on dispose d'un morphisme du groupe (additif) $\mathbb{Z}$ dans G, $\Gamma_x : \mathbb{Z} \longrightarrow G$ défini par $\Gamma_x(m) = x^m$.

Proposition 1.1.13 – *Soient G et G' deux groupes dont les éléments neutres sont respectivement notés e et e' et $\phi : G \longrightarrow G'$ un morphisme de groupes de G dans G'. Alors,*
1. $\phi(e) = e'$;
2. pour tout $g \in G$, $\phi(g^{-1}) = \phi(g)^{-1}$;
3. si H est un sous groupe de G, alors $\phi(H) := \{\phi(g),\, g \in H\}$ est un sous-groupe de G' ;
4. si H' est un sous groupe de G', alors $\phi^{-1}(H') := \{g \in G \,|\, \phi(g) \in H'\}$ est un sous-groupe de G.

Démonstration : Exercice. ∎

Proposition 1.1.14 – *Soient G et G' deux groupes et $\phi : G \longrightarrow G'$ un isomorphisme de groupes de G dans G'. Alors, ϕ^{-1} est un morphisme de groupes de G' dans G.*

Démonstration : Exercice. ∎

Définition 1.1.15 – *Soient G et G' deux groupes dont les éléments neutres sont respectivement noté e et e' et $\phi : G \longrightarrow G'$ un morphisme de groupes de G dans G'. On appelle noyau de ϕ l'ensemble, noté* $\ker(\phi)$*, des éléments de G dont l'image est e'. On appelle image de ϕ l'ensemble, noté* $\mathrm{im}(\phi)$*, des éléments de G' qui sont l'image d'un élément de G. Ainsi,*

$$\ker(\phi) := \{g \in G \,|\, \phi(g) = e'\} \qquad et \qquad \mathrm{im}(\phi) := \phi(G).$$

Proposition 1.1.16 – *Soient G et G' deux groupes et $\phi : G \longrightarrow G'$ un morphisme de groupes de G dans G'. Le noyau de ϕ est un sous-groupe de G et l'image de ϕ est un sous-groupe de G'.*

Démonstration : Le fait que $\ker(\phi)$ soit un sous-groupe de G est un cas particulier du point 4 de la proposition 1.1.13 (avec $H'=\{e'\}$). Le fait que $\mathrm{im}(\phi)$ soit un sous-groupe de G' est un cas particulier du point 3 de la proposition 1.1.13 (avec $H=G$). ∎

La proposition suivante, bien que très simple à démontrer, est extrèmement importante.

Proposition 1.1.17 – *Soient G et G' deux groupes et $\phi : G \longrightarrow G'$ un morphisme de groupes de G dans G'. Le morphisme ϕ est injectif si et seulement si* $\ker(\phi) = \{e\}$.

Démonstration : Supposons que ϕ soit injectif, alors e' (le neutre de G') a au plus un antécédent et c'est e. Comme $\ker(\phi)$ est l'ensemble des antécédents de e, on a bien $\ker(\phi) = \{e\}$. Réciproquement, supposons que $\ker(\phi) = \{e\}$; soient alors g et h deux antécédents d'un même élément $g' \in G'$. Puisque $g' = \phi(g) = \phi(h)$, on a $\phi(g)\phi(h)^{-1} = e'$, c'est-à-dire $\phi(gh^{-1}) = e'$. Ainsi, $gh^{-1} \in \ker(\phi) = \{e\}$. Donc, $gh^{-1} = e$, ce qui prouve que $g = h$. Ainsi, un élément de G a au plus un antécédent par ϕ, ce qui signifie que ϕ est injective. ∎

Exemple 1.1.18 – On reprend les exemples de 1.1.12 pour décrire leurs noyaux et images.
1. L'application $\exp : \mathbb{C} \longrightarrow \mathbb{C}^*$ a pour noyau $2i\pi\mathbb{Z}$ et pour image $\mathbb{C}^*$.
2. L'application $|.| : \mathbb{C}^* \longrightarrow \mathbb{R}_+^*$ admet le cercle unité pour noyau et $\mathbb{R}_+^*$ pour image.

1.2 Familles génératrices ; groupes cycliques.

Soit G un groupe. À toute famille $\mathcal{F} = \{g_i\}_{i\in I}$, indexée par un ensemble non vide I, d'éléments de G on associe l'ensemble suivant, noté $\langle\mathcal{F}\rangle$, et défini par

$$\langle\mathcal{F}\rangle = \{g_{i_1}^{m_1} \dots g_{i_k}^{m_k} \mid k \in \mathbb{N}^*,\, i_1, \dots, i_k \in I,\, m_1, \dots, m_k \in \mathbb{Z}\}.$$

Ainsi, $\langle\mathcal{F}\rangle$ est l'ensemble de tous les éléments de G qui peuvent s'écrire sous la forme d'un produit dont les facteurs sont des éléments de $\mathcal{F}$ ou des inverses d'éléments de $\mathcal{F}$.

Par convention, si $\mathcal{F}$ est indéxée par l'ensemble vide, on pose que $\langle\mathcal{F}\rangle = \{e\}$ (ou e désigne le neutre de G).

Proposition 1.2.1 – *Soit G un groupe (noté multiplicativement) ; pour toute famille $\mathcal{F}$ d'éléments de G, $\langle\mathcal{F}\rangle$ est un sous-groupe de G.*

Démonstration : On peut supposer que l'ensemble d'indexation de $\mathcal{F}$ est non vide car dans le cas contraire le résultat est clair. Posons $\mathcal{F} = \{g_i\}_{i\in I}$, I non vide. Ainsi, il existe un élément s de $\mathcal{F}$ et $e = s^0 \in \langle\mathcal{F}\rangle$. Il est clair que le produit de deux éléments de $\langle\mathcal{F}\rangle$ est encore dans $\langle\mathcal{F}\rangle$. Enfin, soit $g_{i_1}^{m_1} \dots g_{i_k}^{m_k} \in \langle\mathcal{F}\rangle$ ($k \in \mathbb{N}^*$, $i_1, \dots, i_k \in I$ et $m_1, \dots, m_k \in \mathbb{Z}$). Alors, l'inverse de $g_{i_1}^{m_1} \dots g_{i_k}^{m_k}$ dans G, qui est $g_{i_k}^{-m_k} \dots g_{i_1}^{-m_1}$, est bien un élément de $\langle\mathcal{F}\rangle$. Ainsi, $\langle\mathcal{F}\rangle$ est un sous-groupe de G. ∎

Définition 1.2.2 – *Soit G un groupe ; pour toute famille $\mathcal{F}$ d'éléments de G, le sous-groupe $\langle\mathcal{F}\rangle$ de G est appelé sous-groupe engendré par S.*

Le procédé de construction de $\langle\mathcal{F}\rangle$ à partir de la famille $\mathcal{F}$ est très simple : on a mis dans $\langle\mathcal{F}\rangle$ tous les éléments indispensables (et seulement eux) pour faire de $\langle\mathcal{F}\rangle$ un sous-groupe de G contenant les éléments de $\mathcal{F}$. En un certain sens, on a construit *le plus petit sous-groupe de G contenant les éléments de $\mathcal{F}$*. Cette idée est précisée par la proposition suivante.

Proposition 1.2.3 – *Soit G un groupe ; pour toute famille $\mathcal{F}$ de G, $\langle\mathcal{F}\rangle$ est l'intersection de tous les sous-groupes de G contenant les éléments de $\mathcal{F}$.*

Démonstration : On note H l'intersection de tous les sous-groupes de G contenant les éléments de $\mathcal{F}$; en vertu de la proposition 1.1.10, c'est un sous-groupe de G. Bien sûr, H contient les éléments de $\mathcal{F}$. Puisque H est un sous-groupe de G qui contient les éléments de $\mathcal{F}$, il doit contenir e, tous les éléments de $\mathcal{F}$ ainsi que leurs inverses et tous les produits des ces éléments. Ceci assure que H contient $\langle\mathcal{F}\rangle$. Réciproquement, d'après 1.2.1, $\langle\mathcal{F}\rangle$ est un sous-groupe de G qui contient les éléments de $\mathcal{F}$. À ce titre, il contient l'intersection des sous-groupes de G qui contiennent les éléments de $\mathcal{F}$; c'est-à-dire que $H \subseteq \langle\mathcal{F}\rangle$. ∎

Définition 1.2.4 – *Soit G un groupe ; une famille $\mathcal{F}$ d'éléments de G telle que $\langle\mathcal{F}\rangle = G$ est appelée famille génératrice de G.*

Les groupes qui admettent une famille génératrice réduite à un seul élément sont particulièrement simples.

Définition 1.2.5 – *Si G est un groupe et si il existe $x \in G$ tel que G soit engendré par $\{x\}$, on dit que G est un groupe monogène.*

Remarque 1.2.6 –
1. Si $\mathcal{F} = \{s_1, \ldots, s_t\}$ est une famille finie d'éléments de G, le sous-groupe engendré par cette famille (que l'on appellera aussi sous-groupe de G engendré par $s_1, \ldots, s_t$), sera souvent noté $\langle s_1, \ldots, s_t\rangle$ au lieu de $\langle\mathcal{F}\rangle$.
2. Si x est un élément de G, le sous-groupe engendré par x est l'ensemble $\langle x\rangle = \{x^i \,|\, i \in \mathbb{Z}\}$. En particulier, si G est un groupe monogène, il est abélien.
3. Il convient de remarquer que, si le groupe G est noté additivement au lieu d'être noté multiplicativement, quelques modifications sont à apporter à ce qui précède. En particulier, le neutre de G sera souvent noté 0. De plus, si x est un élément de G, l'inverse de x est noté $-x$ (et non plus x^{-1}), l'élément de G obtenu en "composant" (c'est-à-dire ici en additionnant) n copies de x ($n \in \mathbb{N}^*$) est noté $nx = x + \ldots + x$ (n fois). On peut étendre ceci aux entiers négatifs en posant $(-n)x = (-x) + \ldots + (-x) = -(nx)$ ($n \in \mathbb{N}^*$). Enfin, on pose $0x = 0$ (de même que l'on avait $x^0 = e$ en notation multiplicative). Là encore, pour $m, m' \in \mathbb{Z}$ et $x \in G$, on a $mx + m'x = (m + m')x$. Plus généralement, si $\mathcal{F} = \{g_i\}_{i\in I}$ est une famille de G indexée par l'ensemble non vide I, le sous-groupe $\langle\mathcal{F}\rangle$ engendré par $\mathcal{F}$ devient

$$\langle S\rangle = \{m_1 g_{i_1} + \ldots + m_k g_{i_k} \,|\, k \in \mathbb{N}^*,\, i_1, \ldots, i_k \in I,\, m_1, \ldots, m_k \in \mathbb{Z}\}.$$

Ceci ne change rien à tout ce qui précède sauf, évidemment, la notation.
4. Le groupe (additif) $\mathbb{Z}$ est cyclique puisqu'il est engendré par 1. En effet, conformément au point 3 de la présente remarque, $\langle 1\rangle = \{m1 \,|\, m \in \mathbb{Z}\} = \mathbb{Z}$.

Théorème 1.2.7 – *Tout sous-groupe d'un groupe monogène est monogène.*

Démonstration : Soit G un groupe monogène. Il existe $x \in G$ tel que $G = \langle x\rangle$. Soit H un sous-groupe de G. Si $H = \{e\}$, il est monogène engendré par e. Sinon, l'ensemble $\{n \in \mathbb{N}^* \,|\, x^n \in H\}$ est non vide et, à ce titre, il contient un plus petit élément m. Nous allons montrer que x^m engendre H. Soit $y \in H$; puisque G est engendré par x, il existe $n \in \mathbb{Z}$ tel que $y = x^n$. La division euclidienne de n par m fournit un couple (q, r) tel que $q \in \mathbb{Z}$, $r \in \{0, \ldots, m-1\}$ et $n = mq + r$. Il s'ensuit que $y = x^n = x^{mq+r} = (x^m)^q x^r$. Donc, $x^r = (x^m)^{-q} y \in H$. Mais, puisque $r \in \{0, \ldots, m-1\}$, la définition de m impose que $r = 0$. Ainsi, $y = (x^m)^q$. On a donc montré que $H \subseteq \langle x^m\rangle$. L'inclusion inverse est évidente, de sorte que $H = \langle x^m\rangle$: H est monogène. ∎

On termine cette sous-section avec la définition de la notion d'ordre. Il s'agit simplement d'un point de vocabulaire destiné à simplifier les énoncés à venir. La proposition 1.2.9 est néanmoins très importante.

Définition 1.2.8 –
1. On dit qu'un groupe G est d'ordre infini si il contient une infinité d'éléments. Si un groupe G contient un nombre fini d'éléments, on dit que G est un groupe fini et l'ordre de G est le nombre d'éléments de G. L'ordre d'un groupe G sera noté $|G|$.
2. Soit x un élément du groupe G, on appelle ordre de x l'ordre du sous-groupe $\langle x\rangle$ de G engendré par x.

Proposition 1.2.9 – *Soit G un groupe (noté multiplicativement) et x un élément de G.*
1. L'ordre de x est fini si et seulement si il existe $m > 0$ tel que $x^m = e$.
2. Si l'ordre de x est fini, c'est le plus petit entier $n > 0$ tel que $x^n = e$ et alors, $\langle x\rangle = \{e, x, \ldots, x^{n-1}\}$.

Démonstration : 1. ($\Longrightarrow$) On suppose l'ordre de x fini ; alors, l'ensemble $\langle x\rangle = \{x^i \,|\, i \in \mathbb{Z}\}$ est fini et par suite il existe $i, j \in \mathbb{Z}$, $i < j$, tels que $x^i = x^j$. Il s'ensuit que $x^{j-i} = e$ avec $j - i > 0$. Ce qui montre l'implication.
($\Longleftarrow$) On suppose qu'il existe $m > 0$ tel que $x^m = e$. L'ensemble des entier $p > 0$ tels que $x^p = e$ est donc non vide et, à ce titre, il contient un plus petit élément que l'on note n. De plus, si m est un entier quelconque dans $\mathbb{Z}$, on peut procéder à la division euclidienne de m par n et obtenir deux entiers q et r tels que $0 \leq r < n$ pour lesquels $m = qn + r$. Il vient alors que $x^m = x^{qn+r} = x^{qn}x^r = (x^n)^q x^r = x^r$ de sorte que x^m est présent dans la liste $e, x, \ldots, x^{n-1}$ (remarquez par exemple que $x^{-1} = x^{n-1}$). Ceci montre que $\langle x\rangle \subseteq \{e, x, \ldots, x^{n-1}\}$. Comme l'inclusion en sens inverse est évidente, on a montré que $\langle x\rangle = \{e, x, \ldots, x^{n-1}\}$. Ceci clos la preuve de la seconde implication. De plus, la liste $e, x, \ldots, x^{n-1}$ est sans répétitions. En effet, dans le cas contraire, il existerait un couple d'entiers (i, j) tel que $0 \leq i < j \leq n - 1$ et $x^{j-i} = e$. Comme $0 < j - i < n$, ceci contredirait le choix minimale de n. On en déduit que l'ordre de x est bien n, ce qui prouve le second point. ∎

Exemple 1.2.10 – Le groupe $\mathbb{Z}$ est un groupe (monogène) d'ordre infini.

1.3 *Exercices.*

Exercice 1.3.1 – Soit G un groupe (noté multiplicativement) et H un sous-ensemble de G. Montrer que H est un sous-groupe de G si et seulement si $H \neq \emptyset$ et pour tout couple (a, b) d'éléments de H, $ab^{-1} \in H$.

Exercice 1.3.2 – Soit G un groupe.
1. A tout élément $a \in G$ on associe le centralisateur de a dans G, noté $Z(a)$, qui est l'ensemble des élément de G qui commutent avec a. Montrer que, pour tout a dans G, $Z(a)$ est un sous-groupe de G.
2. On appelle centre de G le sous-ensemble de G, noté $Z(G)$, des éléments de G qui commutent avec tout élément de G. Montrer que le centre de G est un sous-groupe de G.

Exercice 1.3.3 – **Racines complexes de l'unité.** On note $U_1(\mathbb{C})$ l'ensemble des complexes de module 1.
1. Montrer que $U_1(\mathbb{C})$ est un sous-groupe de $\mathbb{C}^*$ muni de la multiplication des complexes. Ce

groupe s'appelle le groupe unimodulaire complexe.
2. On considère l'ensemble μ des complexes $z \in \mathbb{C}$ pour lesquels il existe un entier $n \in \mathbb{N}^*$ tel que $z^n = 1$. Ainsi,

$$\mu := \{z \in \mathbb{C} \,|\, \exists n \in \mathbb{N}^*,\, z^n = 1\}.$$

Montrer que l'ensemble μ muni de la multiplication des nombres complexes est un sous-groupe du groupe unimodulaire complexe.
3. Soit $p \in \mathbb{N}^*$; on note μ_p l'ensemble des complexes racines p-èmes de l'unité : $\mu_p := \{z \in \mathbb{C} \,|\, z^p = 1\}$. Montrer que μ_p est un sous-groupe de μ et dresser la liste des éléments de μ_p. Montrer que μ_p est un groupe cyclique et déterminer tous les éléments de μ_p qui engendrent μ_p.

Exercice 1.3.4 – Soient G et G' deux groupes, et $\phi : G \longrightarrow G'$ un morphisme de groupes de G dans G'.
1. Montrer que si $x \in G$ est d'ordre fini n, alors $\phi(x)$ est d'ordre fini m et que m divise n.
2. On suppose que ϕ est un isomorphisme ; montrer que $x \in G$ est d'ordre fini n si et seulement si $\phi(x)$ est d'ordre fini n.
3. Donner un exemple de morphisme tel qu'un élément d'ordre infini ait pour image un élément d'ordre fini.
4. Donner un exemple d'isomorphisme entre un groupe G et un de ses sous-groupes propres (c'est-à-dire distinct de $\{e\}$ et de G).
5. Montrer que deux groupes d'ordre infini ne sont pas nécessairement isomorphes. (Indication : on pourra montrer qu'il n'existe pas d'isomorphisme entre le groupe additif $\mathbb{Q}$ et le groupe multiplicatif $\mathbb{Q}_+^*$ en utilisant l'irrationnalité de $\sqrt{2}$.)

Exercice 1.3.5 – **Théorème de Lagrange.**
Soit G un groupe fini.
1. Soit H un sous groupe de G.
1.1. On considère la relation binaire $\mathcal{R}$ définie sur G par : pour $g, h \in G$, $g\mathcal{R}h$ si il existe $k \in H$ tel que $g = hk$. Montrer que $\mathcal{R}$ est une relation d'équivalence et décrire ses classes.
1.2. Montrer que l'ordre de H divise l'ordre de G (théorème de Lagrange).
2. Soit $g \in G$. Montrer que $g^{|G|} = e$, où e est le neutre de G.

2 *La notion d'anneau ; la notion de corps.*

Un anneau est un ensemble muni de deux lois de composition interne (l'une sera notée additivement et l'autre multiplicativement), qui sont liées l'une à l'autre par une condition de compatibilité (appelée distributivité).

2.1 Définitions fondamentales.

Définition 2.1.1 – *Soient A un ensemble, $+$ et $\times$ deux lois de composition interne sur A. On dit que $(A, +, \times)$ est un anneau (d'addition $+$ et de multiplication $\times$) si les conditions suivantes sont satisfaites.*
1. $(A, +)$ est un groupe abélien (dont le neutre, noté 0, est appelé l'élément nul de A).
2. La loi $\times$ est associative (i.e. $\forall a, b, c \in A$, $a \times (b \times c) = (a \times b) \times c$).
3. La loi $\times$ admet un élément neutre (i.e. un élément e tel que $\forall a \in A$, $e \times a = a \times e = a$).
4. La loi $\times$ est distributive par rapport à la loi $+$ (i.e. $\forall a, b, c \in A$, on a $a \times (b+c) = a \times b + a \times c$ et $(b + c) \times a = b \times a + c \times a$).

Définition 2.1.2 – *Un anneau $(A, +, \times)$ est dit commutatif s'il vérifie la propriété suivante :*
5. Pour a et b dans A, on a $a \times b = b \times a$.

Remarque 2.1.3 – Soit $(A, +, \times)$ un anneau.
1. Si a et b sont dans A, on note souvent ab au lieu de $a \times b$ pour simplifier l'écriture.
2. Comme on le vérifie aisément, un anneau admet un unique élément neutre pour la multiplication. Il est noté 1 et appelé l'élément unité (ou l'unité) de A. Lorsqu'il y a un risque de confusion, on note 1_A l'unité de l'anneau A.
3. On déduit facilement des définitions les résultats suivants : pour a et b dans A, $0a = a0 = 0$ et $a(-b) = (-a)b = -(ab)$. Leur démonstration est laissée en exercice.
4. Compte tenu du fait que, par définition, un groupe est un ensemble non vide, un anneau doit aussi être non vide.
5. Tout ensemble $A = \{a\}$ réduit à un seul élément peut être muni d'une structure d'anneau de façon évidente. Il est clair alors que l'élément nul et l'élément unité de A sont égaux. Réciproquement, si A est un anneau dont l'élément nul et l'élément unité de A coïncident, alors A est réduit à un seul élément comme on le déduit facilement du point 3 ci-dessus. Désormais, on appelera anneau non nul tout anneau A non réduit à un singleton.

Définition 2.1.4 – *Un anneau $(A, +, \times)$ est dit intègre s'il est non nul et vérifie la propriété suivante : pour a et b dans A, $ab = 0$ entraîne que a ou b est nul.*

Exemple 2.1.5 – Les exemples suivants sont célèbres, on laisse en exercice la preuve des affirmations avancées.
(1) $(\mathbb{Z}, +, \times)$ est un anneau intègre et commutatif.
(2) Si $\mathbb{K}$ désigne $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, l'ensemble $\mathbb{K}$ muni des lois d'addition et de multiplication usuelles est un anneau commutatif intègre.
(3) Si $\mathbb{K}$ désigne $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, pour tout entier $n > 1$, $(M_n(\mathbb{K}), +, \times)$ est un anneau qui n'est ni commutatif ni intègre.

Remarque 2.1.6 – Soit $(A, +, \times)$ un anneau. Un élément a de A est dit inversible s'il admet un symétrique pour la loi $\times$, c'est-à-dire si il existe un élément $a' \in A$ tel que $aa' = a'a = 1$. On montre facilement que si un élément a de A est inversible, il existe un unique $a' \in A$ tel que $aa' = a'a = 1$; cet élément est noté a^{-1}. Un élément inversible de A est parfois appelé *une unité* de A (attention à la confusion avec 1_A l'unité de A). L'ensemble des éléments inversibles de A (ou unités de A) est noté $U(A)$. On vérifie facilement que $(U(A), \times)$ est un groupe dont 1_A est l'élément neutre ; ce groupe s'appelle groupe des unités de $(A, +, \times)$. Si $\mathbb{K}$ est $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, le groupe des unités de $(\mathbb{K}, +, \times)$ est $(\mathbb{K} \setminus \{0\}, \times)$, celui de $(\mathbb{Z}, +, \times)$ est $(\{-1, 1\}, \times)$. Le groupe des unités de $(M_n(\mathbb{K}), +, \times)$ est le groupe général linéaire des matrices inversibles : $(GL_n(\mathbb{K}), \times)$.

Définition 2.1.7 – *On appelle corps un anneau $(A, +, \times)$ non nul dont tout élément différent de 0 est inversible, c'est-à-dire tel que $U(A) = A \setminus \{0\}$.*

Exemple 2.1.8 – Il est clair que si $\mathbb{K}$ est $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, $(\mathbb{K}, +, \times)$ est un corps. En revanche, $(\mathbb{Z}, +, \times)$ n'est pas un corps puisque $U(\mathbb{Z}) = \{-1, 1\}$.

On rappelle le point suivant, déjà mentionné dans la section 1 de ce chapitre. Pour tout élément $a \in A$, si $n \in \mathbb{Z}$, on pose $na = a + \ldots + a$, n-fois si $n > 0$, $0a = 0$ et $na = (-a) + \ldots + (-a)$, $-n$-fois si $n < 0$. Pour $m, n \in \mathbb{Z}$, on a alors $(m + n)a = ma + na$.

En oute, pour tout élément $a \in A$, si $n \in \mathbb{N}^*$, on pose $a^n = a \ldots a$, n-fois. De plus, par convention, on pose $a^0 = 1$. Pour $m, n \in \mathbb{N}$, on a alors $a^{m+n} = a^m a^n$. Si $a \in A$ est un élément

inversible et si n est un entier strictement négatif, on pose $a^n = (a^{-1})^{-n}$. Pour $m, n \in \mathbb{Z}$, on a alors $a^{m+n} = a^m a^n$.

L'énoncé suivant est connu sous le nom de *formule du binôme*.

Proposition 2.1.9 – *Soient $(A, +, \times)$ un anneau et n un entier non nul. Si a et b sont deux éléments de A qui commutent (c'est-à-dire que $ab = ba$), alors :*

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

Démonstration : La preuve procède par récurrence sur n. Le résultat est trivial pour $n = 1$. On suppose la formule vraie au rang n. Alors, puisque a et b commutent, on a :

$$(a+b)^{n+1} = (a+b)^n(a+b) = (\sum_{k=0}^{n} C_n^k a^k b^{n-k})(a+b) = \sum_{k=0}^{n} C_n^k a^{k+1} b^{n-k} + \sum_{k=0}^{n} C_n^k a^k b^{n+1-k}.$$

Un changement d'indice $k+1 = h$ dans la première somme et $k = h$ dans la seconde conduit à :

$$(a+b)^{n+1} = \sum_{h=1}^{n+1} C_n^{h-1} a^h b^{n+1-h} + \sum_{h=0}^{n} C_n^h a^h b^{n+1-h} = C_n^0 b^{n+1} + \sum_{h=1}^{n} (C_n^{h-1} + C_n^h) a^h b^{n+1-h} + C_n^n a^{n+1}.$$

Comme $C_n^0 = C_{n+1}^0 = 1$ et $C_n^n = C_{n+1}^{n+1} = 1$ et comme de plus $C_n^{h-1} + C_n^h = C_{n+1}^h$, il vient :

$$(a+b)^{n+1} = C_{n+1}^0 b^{n+1} + \sum_{h=1}^{n} C_{n+1}^h a^h b^{n+1-h} + C_{n+1}^{n+1} a^{n+1} = \sum_{h=0}^{n+1} C_{n+1}^h a^h b^{n+1-h}.$$

Ceci achève la preuve. ∎

L'étude des anneaux non-commutatifs présente des difficultés spécifiques. De plus, elle ne fait pas partie des buts de ce cours. Dans la suite, nous nous limiterons donc au cas commutatif. Ceci exclut, entre autres, le cas des anneaux de matrices. Afin d'éviter d'incessantes répétitions, nous décidons qu'**à partir de maintenant, sauf mention expresse du contraire, *anneau* signifie *anneau commutatif***.

On définit à présent les *sous-structures* associées à la structure d'anneau. Bien sûr, en analogie avec les groupes, on s'attend à devoir introduire une notion de sous-anneau. En fait, il y a une autre sous-structure, plus intéressante, appelée idéal.

Définition 2.1.10 – *Soient $(A, +, \times)$ un anneau et B un sous-ensemble de A. On dit que B est un sous-anneau de A si il vérifie les conditions suivantes.*
1. B est un sous-groupe de $(A, +)$.
2. 1_A est dans B.
3. Si a et b sont dans B, alors ab est dans B.

Exemple 2.1.11 – Il est clair que $\mathbb{Z}$ et $\mathbb{Q}$ sont des sous-anneaux de $(\mathbb{R}, +, \times)$.

Remarque 2.1.12 – Soient $(A, +, \times)$ un anneau et B un sous-anneau de A. Les restrictions à B des lois additive et multiplicative de A définissent des lois de composition interne sur B. Muni de ces lois, B est lui-même un anneau.

On en vient, à présent, à la notion d'idéal.

Définition 2.1.13 – *Soit $(A,+,\times)$ un anneau. Un sous-ensemble I de A est appelé un idéal s'il vérifie les conditions suivantes :*
1. I est un sous-groupe de $(A,+)$;
2. pour $a \in A$ et $x \in I$, on a $ax \in I$.

Remarque 2.1.14 – Soit $(A,+,\times)$ un anneau.
1. Les sous-ensembles $\{0\}$ et A sont des idéaux de A.
2. Si A est un corps, $\{0\}$ et A sont les seuls idéaux de A. En effet, si I est un idéal de A non réduit à 0, il contient un élément non nul $a \in A$. Comme a est non nul, c'est une unité de A et il existe donc un inverse a^{-1} de a. On a alors $a^{-1}a = 1 \in I$. Il s'ensuit que tout élément $b \in A$ est dans I puisque $b = b1$.

Exemple 2.1.15 – Les idéaux d'un anneau quelconque peuvent être très variés. Cependant, les idéaux de $\mathbb{Z}$ sont très simples à décrire.
1) Si $a \in \mathbb{Z}$, il est facile de vérifier que l'ensemble $a\mathbb{Z}$ des multiples de a est un idéal de $\mathbb{Z}$.
2) En fait, les idéaux de $\mathbb{Z}$ sont tous de la forme mentionnée au 1). En effet, un idéal I est en particulier un sous-groupe de $\mathbb{Z}$ et on sait que tout sous-groupe de $\mathbb{Z}$ est de la forme $a\mathbb{Z}$ pour un certain $a \in \mathbb{Z}$.

Proposition 2.1.16 – *Soient A un anneau, $\mathcal{I}$ un ensemble non vide et $\{I_i\}_{i\in\mathcal{I}}$ une famille d'idéaux de A. Alors $\cap_{i\in\mathcal{I}} I_i$ est un idéal de A.*

Démonstration : Pour $i \in \mathcal{I}$, I_i est un sous-groupe de A et donc $\cap_{i\in I} I_i$ est un sous-groupe de A. Par ailleurs, si $a \in A$ et si $b \in \cap_{i\in I} I_i$, pour tout $i \in \mathcal{I}$, ab est dans I_i puisque I_i est un idéal. Il s'ensuit que ab est dans $\cap_{i\in I} I_i$, ce qui achève la preuve. ∎

On aborde à présent les morphismes entre anneaux.

Définition 2.1.17 – *Soient $(A,+,\times)$ et $(B,+,\times)$ deux anneaux et $f : A \longrightarrow B$ une application de A vers B. On dit que f est un morphisme d'anneaux de $(A,+,\times)$ vers $(B,+,\times)$ si les conditions suivantes sont vérifiées.*
1. f est un morphisme de groupes de $(A,+)$ vers $(B,+)$.
2. $f(1_A) = 1_B$.
3. Pour a et b dans A, on a $f(ab) = f(a)f(b)$.
Un morphisme d'anneaux bijectif est appelé un isomorphisme d'anneaux. Un morphisme d'un anneau vers lui-même est appelé un endomorphisme et un endomorphisme bijectif est appelé un automorphisme.

Proposition 2.1.18 – *Soient $(A,+,\times)$ et $(B,+,\times)$ deux anneaux et $f : A \longrightarrow B$ un morphisme d'anneaux de $(A,+,\times)$ vers $(B,+,\times)$. On a les propriétés suivantes.*
1. Si a est une unité de A, alors $f(a)$ est une unité de B et $f(a)^{-1} = f(a^{-1})$.
2. Si J est un idéal de B, l'ensemble $f^{-1}(J) := \{a \in A \,|\, f(a) \in J\}$ est un idéal de A.
3. Si f est surjective et si I est un idéal de A, l'ensemble $f(I) := \{f(a),\, a \in I\}$ est un idéal de B.

Démonstration : Si a est une unité de A, on a $1_B = f(1_A) = f(a^{-1}a) = f(a^{-1})f(a)$ et de même $1_B = f(1_A) = f(aa^{-1}) = f(a)f(a^{-1})$. Le premier point s'ensuit immédiatement. Les deux points suivants sont laissés au lecteur en guise d'exercice. ∎

Définition 2.1.19 – *Soient $(A,+,\times)$ et $(B,+,\times)$ deux anneaux et $f : A \longrightarrow B$ un morphisme d'anneaux de $(A,+,\times)$ vers $(B,+,\times)$. L'ensemble* $\ker(f) := \{a \in A \,|\, f(a) = 0\}$ *est appelé le noyau de f.*

Proposition 2.1.20 – *Soient $(A,+,\times)$ et $(B,+,\times)$ deux anneaux et $f : A \longrightarrow B$ un morphisme d'anneaux de $(A,+,\times)$ vers $(B,+,\times)$. Le noyau* $\ker(f)$ *de f est un idéal de A et l'application f est injective si et seulement si* $\ker(f) = \{0\}$. *De plus, $f(A)$ est un sous-anneau de B.*

Démonstration : Le fait que $\ker(f)$ soit un idéal de A est un cas particulier du second point de la proposition 2.1.18 (avec $J = (0)$). L'application f étant un morphisme des groupes de $(A,+)$ vers $(B,+)$, son injectivité équivaut à $\ker(f) = \{0\}$ conformément aux résultats concernant les groupes. La vérification du fait que $f(A)$ est un sous-anneau de B est laissée en exercice. ∎

On termine par la notion de produit direct d'anneaux.

Proposition 2.1.21 – *Soient $s \in \mathbb{N}^*$ et $A_1, \ldots, A_s$ des anneaux. On définit sur $A := A_1 \times \ldots \times A_s$ deux lois de composition interne $+$ et $\times$ en posant, pour $(a_1, \ldots, a_n)$ et $(b_1, \ldots, b_n) \in A$,*

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n) \text{ et } (a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Muni de ces deux lois de composition interne, $(A,+,\times)$ est un anneau.

Démonstration : Exercice. ∎

Définition 2.1.22 – *Soient $s \in \mathbb{N}^*$ et $A_1, \ldots, A_s$ des anneaux ; l'anneau $A := A_1 \times \ldots \times A_s$, défini en 2.1.21 est appelé produit direct des anneaux $A_1, \ldots, A_s$.*

2.2 Familles génératrices d'un idéal ; anneaux principaux.

Soit A un anneau et $\mathcal{F} = \{x_i\}_{i \in I}$ une famille, indexée par un ensemble non vide I, d'éléments de A. On pose

$$\langle \mathcal{F} \rangle = \{a_1 x_{i_1} + \ldots + a_k x_{i_k},\, k \in \mathbb{N}^*, a_1, \ldots, a_k \in A,\, i_1, \ldots, i_k \in I\}.$$

En outre, si $\mathcal{F}$ est indexée par l'ensemble vide, par convention, on pose $\langle \mathcal{F} \rangle = \{0\}$.

Proposition 2.2.1 – *Soit A un anneau et $\mathcal{F}$ une famille d'éléments de A. Alors, $\langle \mathcal{F} \rangle$ est un idéal de A.*

Démonstration : Exercice. ∎

Définition 2.2.2 – *Soit A un anneau.*
1. Si $\mathcal{F}$ est une famille d'éléments de A, l'idéal $\langle \mathcal{F} \rangle$ de A est appelé l'idéal engendré par $\mathcal{F}$.
2. Si I est un idéal de A, toute famille $\mathcal{F}$ d'éléments de A telle que $\langle \mathcal{F} \rangle = I$ est appelée une famille génératrice de I.

Remarque 2.2.3 – On reprend les notations ci-dessus.
1. Si $\mathcal{F} = \{x_1, \ldots, x_s\}$ est une famille finie de A, l'idéal qu'elle engendre est souvent noté $\langle x_1, \ldots, x_s \rangle$ au lieu de $\langle \mathcal{F} \rangle$.
2. Si $\mathcal{F} = \{0\}$, il est clair que $\langle \mathcal{F} \rangle = \{0\}$.

Définition 2.2.4 – *Soit A un anneau, un idéal qui admet une partie génératrice à un seul élément sera appelé un idéal principal.*

Définition 2.2.5 – *Un anneau est dit principal s'il est intègre et si tous ses idéaux sont principaux.*

Exemple 2.2.6 – Tout idéal de $\mathbb{Z}$ est principal comme on l'a vu à l'exemple 2.1.15 et $\mathbb{Z}$ est intègre. Ainsi, $\mathbb{Z}$ est un anneau principal.

Proposition 2.2.7 – *Soit A un anneau. Pour toute famille $\mathcal{F}$ d'éléments de A, $\langle \mathcal{F} \rangle$ est l'intersection de tous les idéaux de A contenant les éléments de $\mathcal{F}$.*

Démonstration : Exercice. ∎

2.3 *Exercices.*

Exercice 2.3.1 – Montrer que l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$ est un anneau commutatif pour l'addition et la multiplication usuelle des fonctions. Cet anneau est-il intègre ?

Exercice 2.3.2 – Montrer que dans un anneau (non nécessairement commutatif) $(A, +, \times)$, la loi multiplicative ne satisfait pas nécessairement à la propriété de simplification (*i.e.* $\forall a, b \in A$ et $\forall c \in A^*$, $ac = bc \Longrightarrow a = b$ (simplification à droite) et $ca = cb \Longrightarrow a = b$ (simplification à gauche)). Donner des exemples d'anneaux où cette propriété est satisfaite.

Exercice 2.3.3 – Montrer que tout sous-anneau d'un anneau intègre est intègre.

Exercice 2.3.4 – Montrer que l'ensemble, noté $\mathbb{Z}[i] := \mathbb{Z} + i\mathbb{Z}$ des nombres complexes de la forme $a + ib$ avec $a, b \in \mathbb{Z}$ est un sous-anneau de $(\mathbb{C}, +, \times)$. Déterminer l'ensemble des unités de $\mathbb{Z} + i\mathbb{Z}$ (en caractérisant une unité par la valeur de son module).

Exercice 2.3.5 – Montrer que l'ensemble, noté $\mathbb{Z}[\sqrt{2}] := \mathbb{Z} + \sqrt{2}\mathbb{Z}$ des nombres réels de la forme $a + \sqrt{2}b$ avec $a, b \in \mathbb{Z}$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

Exercice 2.3.6 – Montrer que l'ensemble, noté $\mathbb{Q}[\sqrt{2}] := \mathbb{Q} + \sqrt{2}\mathbb{Q}$ des nombres réels de la forme $a + \sqrt{2}b$ avec $a, b \in \mathbb{Q}$ est un corps.

Exercice 2.3.7 – Soit $(A, +, \times)$ un anneau non nécessairement commutatif. Le centre de A, noté $Z(A)$, est l'ensemble des éléments a de A tel que $ab = ba$ pour tout $b \in A$.
1) Montrer que $Z(A)$ est un sous anneau de A.
2) Calculer $Z(M_n(\mathbb{K}))$.

Exercice 2.3.8 – Soient A et B deux anneaux et $f : A \to B$ un morphisme d'anneaux. Montrer que, si f est bijectif, alors f^{-1} est un morphisme d'anneaux.

Exercice 2.3.9 – Soit $(A, +, \times)$ un anneau. Montrer qu'une partie I de A est un idéal de A si et seulement si
1. elle est non vide ;
2. $a \in I$ et $b \in I$ implique $a + b \in I$ (stabilité de I par addition) ;
3. $a \in A$ et $b \in I$ implique $ab \in I$ (stabilité de I par multiplication par tout élément de A).

Exercice 2.3.10 – Soit $(A, +, \times)$ un anneau. Montrer qu'un idéal I de A est égal à A si et seulement si il contient 1.

Exercice 2.3.11 – Soient $(A, +, \times)$ un anneau et I et J deux idéaux de A. On note $I + J$ l'idéal de A engendré par $I \cup J$ et IJ l'idéal de A engendré par l'ensemble S des produits ab où $a \in I$ et $b \in J$. Donner une description (aussi simple que possible) des idéaux $I + J$ et IJ. (**N.B.** Attention, ici IJ n'est pas l'ensemble $\{ab,\, a \in I,\, b \in J\}$!)

Exercice 2.3.12 – Soit A un anneau commutatif non nul. On appelle nilradical de A l'ensemble des éléments *nilpotents* de A, c'est-à-dire l'ensemble des éléments $a \in A$ tels qu'il existe $n \in \mathbb{N}^*$ pour lequel $a^n = 0$. Montrer que le nilradical de A est un idéal de A.

Exercice 2.3.13 – Soit $(A, +, \times)$ un anneau non nul. Montrer que A est un corps si et seulement si (0) et A sont les seuls idéaux de A.

Exercice 2.3.14 – Soient A et B deux anneaux non nuls. Montrer que l'anneau $A \times B$ n'est pas intègre. Soient A et B deux corps. L'anneau $A \times B$ est-il un corps ?

Exercice 2.3.15 – Soit A un anneau.
1. Un idéal P de A est dit premier si $P \neq A$ et si, pour tout couple $(a, b) \in A$, $ab \in P$ entraîne que a ou b est dans P. À quelle condition l'idéal (0) de A est-il premier ? Quels sont les idéaux premiers de $\mathbb{Z}$?
2. Un idéal M de A est dit maximal si $M \neq A$ et si le seul idéal contenant strictement M est A. Montrer que tout idéal maximal est premier.

Exercice 2.3.16 – Soient A et B deux anneaux et $f : A \longrightarrow B$ un morphisme d'anneaux. Montrer que si B est intègre, alors $\ker(f)$ est un idéal premier.

Exercice 2.3.17 – Soient A et B deux anneaux. Montrer que $U(A \times B) \cong U(A) \times U(B)$.

SOLUTIONS D'UNE SELECTION D'EXERCICES.

Solution de l'exercice V.4.1. Réf. : [Rivaud ; p.289] (cf. Licence-Anneaux.pdf).
1. On obtient $P = (X^2+3X)(X^2+3X+1) - 6$.
2. On obtient $P = (X^2 + (1-i)X - 5i)S$.

Solution de l'exercice V.4.2. Réf. : [Rivaud ; p.290] (cf. Licence-Anneaux.pdf).
Le procédé algo. usuel de division euclidienne conduit à s'interesser à $P_n - X^{n-1}\cos(n-1)\phi S$. Or le calcul montre que

$$\begin{aligned}
&P_n - X^{n-1}\cos(n-1)\phi S \\
&\quad = X^{n+1}\cos(n-1)\phi - X^n\cos n\phi - X\cos\phi + 1 - X^{n-1}\cos(n-1)\phi(X^2 - 2X\cos\phi + 1) \\
&\quad = X^{n+1}\cos(n-1)\phi - X^n\cos n\phi - X\cos\phi + 1 \\
&\qquad -(X^{n+1}\cos(n-1)\phi - 2\cos\phi X^n\cos(n-1)\phi + X^{n-1}\cos(n-1)\phi) \\
&\quad = (2\cos\phi\cos(n-1)\phi - \cos n\phi)X^n - X^{n-1}\cos(n-1)\phi - X\cos\phi + 1 \\
&\quad = \cos(n-2)\phi X^n - X^{n-1}\cos(n-1)\phi - X\cos\phi + 1 = P_{n-1}.
\end{aligned}$$

Ainsi, pour $n \geq 1$, $P_n = P_{n-1} - X^{n-1}\cos(n-1)\phi S$. On en déduit par récurrence que

$$P_n = (X^{n-1}\cos(n-1)\phi + \ldots + X\cos\phi + 1)S.$$

Solution de l'exercice V.4.3. Réf. : [LFA ; p.132], [Rivaud ; p.295] (cf. Licence-Anneaux.pdf).
1. On a
1) $P = X^5 + X^4 + 2X^3 - 2X + 3 = (X-2)(X^4 + 3X^3 + 7X^2 + 8X + 6) + X^3 + 6X^2 + 8X + 15$,
2) $X^4 + 3X^3 + 7X^2 + 8X + 6 = (X-3)(X^3 + 6X^2 + 8X + 15) + 17X^2 + 17X + 51$.
La méthode usuelle conduit à chercher lun p.g.c.d. de $X^3 + 6X^2 + 8X + 15$ et $17X^2 + 17X + 51 = 17(X^2 + X + 3)$, mais ceci revient à chercher un p.g.c.d. de $X^3 + 6X^2 + 8X + 15$ et $X^2 + X + 3$, or
3) $X^3 + 6X^2 + 8X + 15 = (X+5)(X^2 + X + 3)$.
Ainsi, un p.g.c.d. de P et S est $X^2 + X + 3$.
2. En suivant l'algorithme d'Euclide, on obtient la suite de divisions euclidiennes :

$$\begin{aligned}
X^5 - X^4 + 2X^3 + 1 &= (X^5 + X^4 + 2X^2 - 1) + (-2X^4 + 2X^3 - 2X^2 + 2) \\
X^5 + X^4 + 2X^2 - 1 &= (X+2)(X^4 - X^3 + X^2 - 1) + X^3 + X + 1 \\
X^4 - X^3 + X^2 - 1 &= (X-1)(X^3 + X + 1) + 0.
\end{aligned}$$

On trouve donc $X^3 + X + 1$ et ses associés.
3. On trouve $(X-2)(X+3)$ et ses associés.

Solution de l'exercice V.4.4. Réf. : [LFA ; p.132] (voir aussi [AF ; p. 266] pour une solution alternative. (cf. Licence-Anneaux.pdf).
1. La division euclidienne dans $\mathbb{N}$ assure l'existence d'un couple (q, r) d'éléments de $\mathbb{N}$ tels que $m = qn + r$ et $0 \leq r < n$. Procédons maintenant à la division euclidienne de $X^M - 1$ par $X^n - 1$ en suivant l'algorithme usuel. On a

$$X^m - 1 = X^{m-n}(X^n - 1) + X^{m-n} - 1 \qquad \text{qui a un sens car } m \geq n.$$

Si $m - n < n$, ceci donne la division cherchée ; notons par ailleurs que dans ce cas, on a $m = n + (m-n)$ avec $m - n < n$, ce qui assure que $q = 1$ et $r = m - n$. Sinon, c'est-à-dire si $m - n \geq n$, on doit continuer le procésus algorithmique :

$$X^{m-n} - 1 = X^{m-2n}(X^n - 1) + X^{m-2n} - 1 \qquad \text{qui a un sens car } m \geq n.$$

Là encore, la suite des événements se partage en deux cas. Si $m - 2n < n$, on a terminé car alors

$$\begin{aligned}
X^m - 1 &= X^{m-n}(X^n - 1) + X^{m-n} - 1 \\
&= X^{m-n}(X^n - 1) + X^{m-2n}(X^n - 1) + X^{m-2n} - 1 \\
&= (X^{m-n} + X^{m-2n})(X^n - 1)(X^n - 1) + X^{m-2n} - 1
\end{aligned}$$

est la division cherchée. À nouveau, on voit que dans ce cas, $m = 2n + m - 2n$ est la division euclidienne de m par n. Sinon, il faut continuer ...
À ce stade, ce qui se produit est devenu clair, le procésus enclanché aura q étapes, la dernière conduisant à écrire

$$X^{m-(q-1)n} - 1 = X^{m-qn}(X^n - 1) + X^{m-qn} - 1 \qquad \text{qui a un sens car } m - qn = r \geq 0.$$

Il faut à présent reprendre le raisonnement de façon propre : on a

$$X^{m-in} - 1 = X^{m-(i+1)n}(X^n - 1) + X^{m-(i+1)n} - 1 \qquad \text{pour } 0 \leq i \leq q-1.$$

La somme de ces q équations donne

$$\sum_{i=0}^{q-1}((X^{m-in} - 1) - (X^{m-(i-1)n} - 1)) = (X^n - 1)\sum_{i=0}^{q-1} X^{m-(i+1)n}.$$

C'est-à-dire que l'on a $(X^m - 1) - (X^{m-qn} - 1) = (X^n - 1)\sum_{i=0}^{q-1} X^{m-(i+1)n}$ qui revient à

$$X^m - 1 = (X^n - 1)\sum_{i=0}^{q-1} X^{m-(i+1)n} + X^r - 1.$$

Cette dernière expression est la division euclidienne cherchée.
2. On peut utiliser l'algorithme d'Euclide en parallèle à (m, n) dans $\mathbb{Z}$ et à $(X^m - 1, X^n - 1)$ dans $K[X]$. On sait que si d est le p.g.c.d. de m et n dans $\mathbb{Z}$, d est le dernier reste non nul de l'algorithme d'Euclide et qu'en fait, on dispose d'un suite $(q_1, r_1), \ldots, (q_s, r_s)$ d'entiers tels que, en posant $m = q_1 n + r_1$, $n = r_0 = q_2 r_1 + r_2$, $r_i = q_{i+2}r_{i+1} + r_{i+2}$ pour $0 \leq i \leq s-2$ et $r_{s-1} = q_{s+1}r_s$, où $0 = d = r_s < \ldots < r_2 < r_1 < n$. La procédure de l'algorithme d'Euclide donne alors une suite de relations $X^m - 1 = Q_1(X^n - 1) + R_1$, $R_O = Q_2 R_1 + R_2, \ldots, R_{s-2} = Q_s R_{s-1} + R_s$ et $R_{s-1} = Q_{s+1}R_s$, où $R_0 = X^n - 1$ et $R_i = X^{r_i} - 1$, pour $1 \leq i \leq s$. Un p.g.c.d. de $X^m - 1$ et $X^n - 1$ est le dernier reste non nul de cette suite et donc $X^d - 1$ est un p.g.c.d. de $X^m - 1$ et $X^n - 1$.
3. On multiplie par $X - 1$, ce qui ramène au p.g.c.d. de $X^8 - 1$ et $X^6 - 1$ qui est $X^2 - 1$. Les p.g.c.d. cherchés sont donc $X + 1$ et ses associés.

Solution de l'exercice V.4.5. Réf. : [RDO ; ex.2.1.12 p. 42] (cf. Licence-Anneaux.pdf).
Il est clair que le polynôme nul est solution et qu'aucun polynôme constant non nul n'est solution. Supposons à présent $n = \deg P \geq 1$; alors, il existe $\alpha \in K$ tel que $nP = (X-\alpha)P'$. Si $n \geq 2$, on en déduit que $n(n-1)P = (X-\alpha)^2 P''$. Plus généralement, on montre par récurrence que, pour $1 \leq m \leq n$, on a $n(n-1)\dots(n-m+1)P = (X-\alpha)^m P^{(m)}$. En particulier, $m = n$ donne $n!P = (X-\alpha)^n an!$ (où a est le coefficient dominant de P). Ainsi, tout polynôme non nul divisible par sa dérivée est de la forme $P = a(X-\alpha)^n$, $a \in K^*$, $\alpha \in K$, $n \in \mathbb{N}^*$. Réciproquement, il est clair que de tels polynômes sont solutions.

Solution de l'exercice V.4.6. Réf. : [LFA ; p.134] (cf. Licence-Anneaux.pdf).
1. On peut supposer S non constant. Le cours assure de l'existence d'un couple $(U', V') \in K[X]\times K[X]$ tel que $U'P+V'S+1$. Si $\deg U' \geq \deg S$, alors en procédant à la division euclidienne de U' par S, on obtient un couple (Q, R) tel que $U' = QS + R$ et $\deg R < \deg S$. Ainsi, on a

$$1 = U'P + V'S = (QS+R)P + V'S = RP + (QP+V')S.$$

En posant $U = R$ et $V = QP + V'$, on a donc $UP + VS = 1$ et $\deg U < \deg S$. Par ailleurs, si l'on suppose $\deg V \geq \deg P$, on a $\deg VS = \deg V + \deg S \geq \deg P + \deg S > \deg P + \deg U = \deg PU$. Il s'ensuit que $0 = \deg(VS + PU) = \deg VS$, d'où $\deg UP = -\infty$, c'est-à-dire $UP = 0$. Il vient alors $VS \in K^*$, ce qui contredit les hypothèses sur P et S. Ainsi, on a bien $\deg V < \deg P$ et le couple cherché est déterminé. Supposons, à présent, qu'il existe deux couples (U, V) et (U', V') satisfaisant aux conditions requises. Alors, on a $1 = UP + VS = U'P + V'S$, donc $(U-U')P = (V'-V)S$. Le lemme de Gauss assure que $S|U-U'$ et $P|V-V'$. Soit $S' \in K[X]$ tel que $U - U' = SS'$, si l'on suppose $S' \neq 0$, il vient $\deg(U-U') = \deg S + \deg S' \geq \deg S$, ce qui contredit $\deg U, \deg U' < \deg S$. Ainsi, $U = U'$ et par suite, $V = V'$.
2. L'algorithme d'Euclide donne :

$$\begin{aligned} X^7 - X - 1 &= X^2(X^5+1) - X^2 - X - 1, \\ X^5 + 1 &= (-X^3 + X^2 - 1)(-X^2 - X - 1) - X, \\ -X^2 - X - 1 &= (X+1)(-X) - 1. \end{aligned}$$

Ceci montre que ces deux polynômes sont premiers entre eux. En fait, on peut tirer plus de ces résultats en isolant chaque reste, on a :

$$\begin{aligned} 1 &= -(X+1)X + X^2 + X + 1, \\ X &= (X^2+X+1)(X^3 - X^2 + 1) - (X^5+1), \\ X^2 + X + 1 &= X^2(X^5+1) - (X^7 - X - 1) \end{aligned}$$

Ce dont on déduit (par repport successif)

$$\begin{aligned} 1 &= -(X+1)((X^2+X+1)(X^3-X^2+1) - (X^5+1)) + X^2 + X + 1 \\ &= -(X+1)(X^2+X+1)(X^3-X^2+1) + (X+1)(X^5+1) + X^2 + X + 1 \\ &= (X^2+X+1)(1 - (X+1)(X^3-X^2+1)) + (X+1)(X^5+1) \end{aligned}$$

puis,

$$\begin{aligned} 1 &= (X^2(X^5+1) - (X^7 - X - 1))(1 - (X+1)(X^3-X^2+1)) + (X+1)(X^5+1) \\ &= -(X^7 - X - 1)(1 - (X+1)(X^3-X^2+1)) + (X^5+1)(X^2(1 - (X+1)(X^3-X^2+1)) + (X+1)) \\ &= (X^7 - X - 1)(X^4 - X^2 + X) + (X^5+1)(-X^6 + X^4 - X^3 + X + 1). \end{aligned}$$

Cette égalité est bien une solution au problème posé.

Solution de l'exercice V.4.7. Réf. : M. Vigué (cf. polynomexo08.pdf).
Facile sur le modèle de la résolution des équations diophantiennes.

Solution de l'exercice V.4.8. Réf. : M. Vigué (cf. polynomexo08.pdf).
Facile si l'on travaille dans $\mathbb{C}$ en utilisant les racines 3-ièmes de l'unité.

Solution de l'exercice V.4.9. Réf. : [Rivaud ; ex. 4, 8, 11, p.299 à 301] (cf. Licence-Anneaux.pdf).
1. Un réel x est racine de P ssi $2x^3 - 5x^2 + 1 = 0$ et $6x^2 - 9x + 3 = 0$; on trouve ainsi que $x = 1/2$. Il s'ensuit facilement que $P = (2X-1)(X-2i-1)(X-i-1)$.
2. Comme P est à coefficients complexes, il admet $1+i$ pour racine ssi il admet $1-i$ pour racine. On peut alors calculer $P(1+i)$ et $P(1-i)$ et conclure. Il est néanmoins plus rapide de remarquer que $i+1$ et $i-1$ sont racines ssi $X^2 - 2X + 2$ divise P. La division euclidienne de P par $X^2 - 2X + 2$ donne $P = (X^2 + 4X + 9)(X^2 - 2X + 2) + (a+10)X + (b-18)$. On trouve donc $a = -10$ et $b = 18$ et du même coup la factorisation souhaitée.
3. Les deux premières équations se ramènent à des équations en X^2 de degré 2. On peut donc déterminer leurs racines complexes (pour la première c'est même un calcul de racines 4-èmes et pour la seconde on se ramène à un calcul de racines cubiques de l'unité). Plus simplement, on peut procéder ainsi : a) $X^4 + 1 = (X^2+1)^2 - 2X^2 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$;
b) $X^4 + X^2 + 1 = (X^2+1)^2 - X^2 = (X^2 + X + 1)(X^2 - X + 1)$.
Pour la troisième, c'est plus délicat, il faut remarquer que $P(i) = 0$. Il s'ensuit que i et $-i$ sont racines de P et donc que $X^2 + 1$ divise P. On trouve alors facilement que $P = (X^2+1)(X^2 - 2X + 2)$.

Solution de l'exercice V.4.10. Réf. : [Lang ; ex.8 p. 126] (cf. Licence-Anneaux.pdf).
Les deux premiers sont facile. Pour le troisième, le plus élégant est une décomposition en carré (à la Gauss) : $X^2 + bX + c = (X^2 + 2b/2X + b^2/4) + c - b^2/4 = (X+b/2)^2 + c - b^2/4 = (X+b/2)^2 - i^2\sqrt{(c-b^2/4)}^2 = (X+b/2 - i\sqrt{(c-b^2/4)})(X+b/2+i\sqrt{(c-b^2/4)})$, ainsi, ce polynôme admet une racine double ssi ses deux racines (dans $\mathbb{C}$) $-b/2 + i\sqrt{(c-b^2/4)}$ et $-b/2 - i\sqrt{(c-b^2/4)}$ sont égales, c'est-à-dire ssi $c - b^2/4 = 0$.

Solution de l'exercice V.4.11. Réf. : [Rivaud ; ex.7 p. 308] (cf. Licence-Anneaux.pdf).
Le calcul de P' et P'' donne $P' = (n+2)nX^{n+1} - (n+1)(n+2)X^n + (n+2)$ et $P'' = (n+2)(n+1)n(X^n - X^{n-1})$. Les racines de P'' sont donc 0 et 1. On constate que 1 est aussi racine de P et de P', de sorte que 1 est d'ordre de multiplicié au moins 3.

Solution de l'exercice V.4.12. Réf. : [Rivaud ; ex.9 p. 309] (cf. Licence-Anneaux.pdf).
On peut dériver jusqu'a tomber sur un polynôme dont on sache calculer les racines, par exemple jusqu'a tomber sur un polynôme d'ordre 2. Bien sûr, cette méthode n'aboutit que si l'une des racines est d'ordre au moins 4 ce qui n'est pas sûr. Soyons plus économiques : toute racine multiple est racine du p.g.c.d. de P et P'. Or, le p.g.c.d. (unitaire) de P et P' est $X^3 - 8X^2 + 21X - 18 = (X-2)(X-3)^2$. On constate alors aisément que $P = (X-2)^2(X-3)^3$.

Solution de l'exercice V.4.13. Réf. : [Lang ; ex.2 p. 125] (cf. Licence-Anneaux.pdf).
Facile.

Solution de l'exercice V.4.14. Réf. : [Lang ; ex.8 p.117], [LFA ; §IV.6 exemples et applications] (cf. Licence-Anneaux.pdf).
Les polynômes P et Q admettent $\overline{1}, \ldots, \overline{p-1}$ pour racines, donc le polynôme $P-Q$ aussi. Mais, il est clair que $P-Q$ est de degré inférieur ou égal à $p-2$. Ainsi $P=Q$. En comparant les termes constants de ces deux polynômes, on obtient que $(-1)^{p-1}\overline{1}\ldots\overline{p-1} = -\overline{1}$. Si p est impair on a l'égalité voulue, sinon $p=2$ et l'égalité précédente donne $\overline{1}\ldots\overline{p-1} = \overline{1} = -\overline{1}$ (car $-\overline{1} = \overline{1}$ dans $\mathbb{F}_2$). Ce qui précède montre la congruence souhaitée.

Solution de l'exercice V.4.15. Réf. : [Rivaud ; 4 p.283] (cf. Licence-Anneaux.pdf).
En utilisant $X^2-1 = (X-1)(X+1)$, on trouve par vérification directe que ce polynôme admet $1, -1 = 14, 4, 11$ pour racines.

Solution de l'exercice V.4.16. Réf. : [LFA ; §IV.5 p.141] (cf. Licence-Anneaux.pdf).
Soit G un sous-groupe fini du groupe $U(K)$ des unités de K et soit r son ordre. Soit m le plus grand entier qui soit l'ordre d'un élément de G. Il s'agit de montrer que $m=r$. Supposons au contraire $m<r$. Les racines du polynôme X^m-1 sont les éléments de $U(K)$ dont l'ordre divise m (un sens est évident l'autre est conséquence immédiate de la division euclienne). Il s'ensuit qu'il existe dans G un élément b dont l'ordre n ne divise pas m (car X^m-1 admet au plus $m<r$ racines distinctes). Soit a un élément de G d'ordre m ; comme G est commutatif, l'ordre de ab est le p.p.c.m. de m et de n. Comme n ne divise pas m, le p.p.c.m. de m et n est strictement plus grand que m, ce qui contredit la définition de m.

Solution de l'exercice V.4.17. Réf. : [LFA ; §IV.6 exemples et applications] (cf. Licence-Anneaux.pdf).
Posons $K = \{a_1, \ldots, a_q\}$ et $P = (X-a_1)\ldots(X-a_q)$. (Notons que $P = X^p - X$; en effet, $X^p - X$ et P admettent tous les éléments de K pour racine et donc leur différence, qui est un polynôme de degré strictement inférieur à q et admet q racines distinctes doit être nul). Soit I le noyau recherché ; il est clair que P est dans I. De plus, un polynôme S est dans I ssi il admet tous les éléments de K pour racines. Par exemple, a_1 est racine de S et donc $(X-a_1)$ divise S : il existe $Q_1 \in K[X]$ tel que $S = Q(X-a_1)$. De même, $X-a_2$ divise S. Comme $X-a_1$ et $X-a_2$ sont irréductibles et évidemment pas associés, ils sont premiers entre eux. Le lemme de Gauss assure donc que $X-a_2$ divise Q_1 : il existe $Q_2 \in K[X]$ tel que $S = (X-a_1)(X-a_2)Q_2$. De proche en proche, on montre que $P|S$. Ainsi, $I=(P)$. Alternativement, on peut argumenter ainsi : I est principal et il existe $N \in K[X]$ tel que $I=(N)$. Puisque N est un polynôme qui admet $a_1, \ldots, a_q$ pour racines et puisque N n'est pas nul, il doit être de degré au moins égal à q. Comme par ailleurs, il divise P, son degré doit être au plus égal à q. Ainsi, P et N ont même degré et sont donc associés. Le morphisme $K[X] \longrightarrow \mathcal{F}(K)$, $P \mapsto \widetilde{P}$ est en fait surjectif. Pour le montrer, on doit considérer certains polynômes particuliers de $K[X]$. Pour $1 \leq i \leq q$, on pose

$$Q_i = \frac{\prod_{j\neq i}(X-a_j)}{\prod_{j\neq i}(a_i-a_j)}.$$

Soit $f \in \mathcal{F}(K)$; si l'on pose $P = f(a_1)Q_1 + \ldots + f(a_q)Q_q$, il est clair que $\varphi(P) = f$.

COMMENTAIRES DE REDACTION.

1 – Le chapitre X avec les définitions brutes des structures de base est à finir de rédiger.

2 – Il faut voir si des ajouts ne sont pas nécessaires, au regard du programme, dans la partie X.1.

3 – Le chapitre I semble convenir tel quel. On pourrait ajouter un exercice qui ferait écho à l'exercice 4.15 et à la remarque 2.3.4 du chapitre I et qui montrerait que l'idée de rendre injective une application en restreignant l'ensemble de départ à un système de représentant des fibres n'est pas satisfaisante car arbitraire et ne permet pas de retrouver l'application de départ.

4 – Le chapiter V a été pris d'un vieux cours de Licence et adapté. Il a été relu une fois et corrigé. Il semble donc très fiable.

5 – Les exercices 6.33, 6.34 et 6.35 du chapitre VII ont été relus et sont fiables.

6 – J'ai commencé le nettoyage de l'exercice 6.30 du chapitre VII. Il reste à terminer.

7 – Je parle parfois de sous-ensemble et parfois de parties. Il faut voir comment rendre cela cohérent. D'autant que je ne crois pas avoir défini ce qu'est une partie.

8 – **Ajouts indispensables.** Il faut absolument montrer la compatibilité de la relation d'ordre de $\mathbb{N}$ avec l'addition et la multiplication (cf. Partie II). C'est utile dans certaines démonstrations des résultats admis. Il faut faire de même pour $\mathbb{Z}$ (cf. Partie III). Là aussi, c'est utile dans certaines démonstrations cruciales.

9 – **Ajouts indispensables.** Il faut absolument relire en entier la partie II pour vérifier sa cohérence logique. Je n'ai pas de doute sur l'ensemble, mais il pourrait être utile d'ajouter certains détails intermédiaires.

10 –
1) Il serait souhaitable de nettoyer la partie III en faisant un usage systématique du vocabulaire sur les ensembles et les anneaux (relation d'équivalence, idéal, etc) introduits dans la partie I ou dans les lexiques plutôt que de redéfinir tout naïvement à chaque fois. Le texte s'en trouverait salutairement allégé.
2) Il y a quelques incohérences entre la présentation de l'arithmétique de $\mathbb{Z}$ et celle de $\mathbb{K}[X]$. Par exemple, le p.g.c.d. n'est introduit, dans $\mathbb{Z}$, que pour deux éléments, etc Il faudrait réduire au maximum ces différences. Le point de vue, cependant, est très cohérent.

11 – **Ajouts indispensables.** Il faut absolument compléter le Chapitre VI, Section 2 en ajoutant des démonstrations.

12 – La section sur les algèbres (Chapitre 1, Section 3) me semble contenir ce qui est nécessaire pour la réduction des endomorphismes. Les notions de polynômes minimaux, caractéristiques, etc pourront être définis dans la section sur le réduction.

13 – On pourrait peut-être ajouter aux exercices d'arithmétique des exercices sur les triplets pythagoriciens.

14 – Il faut ajouter à la partie V une section sur la décomposition en facteurs irréductibles dans $\mathbb{C}[X]$ (d'Alembert) et $\mathbb{R}[X]$. Tout cela est dans mon cours de Licence 1 de Saint-Etienne (pour les fonctions polynomiales). Ce serait bien de voir si l'on peut mettre en exercices quelques exemples de polynômes irréductibles de degrés arbitraires de $\mathbb{Q}[X]$ pour souligner le contraste (il pourrait être utile de mettre le critère d'Eisenstein dans le coup).

15 – On peut ajouter (par exemple en appendice) une partie sur les nombres complexes. Le chapitre 4 de mon cours de Licence 1 de Saint-Etienne devrait faire l'affaire.

ETAT DE LA RELECTURE.

1 – La partie I a été relue et est satisfaisante en l'état.

2 – La partie II a été relue très brièvement. Elle semble satisfaisante en l'état, mais une relecture systématique s'impose.

3 – La partie III a été relue rapidement. Elle semble très satisfaisante en l'état, mais une relecture d'ensemble est souhaitable.

4 – La partie X.1 a été relue et est satisfaisante en l'état.

5 – La partie X.2 a été relue et est satisfaisante en l'état.