I. Applications

Soient E et F des ensembles. Se donner une *application* f de E dans F c'est associer à tout élément x de E un unique élément y de F. On note alors

$$\begin{aligned} f : E &\longrightarrow F \\ x &\longmapsto f(x) = y \end{aligned}$$

E est *l'ensemble de départ de* f, F est *l'ensemble d'arrivée* de f et $f(x)$ est *l'image* de x par f. On dit aussi que f *envoie* x sur $f(x)$.

On utilise parfois souvent le terme fonction *fonction* à la place d'*application*.

La manière la plus simple de définir une application f de E dans F est de donner une "formule" permettant de calculer y à partir de x.

Exemple.

– L'application de $\mathbb{R}$ dans $\mathbb{R}$ qui envoie tout réel sur son carré :

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2 \end{aligned}$$

– L'application de $\mathbb{R}_+$ dans $\mathbb{Z}$ qui envoie tout réel positif sur sa partie entière :

$$\begin{aligned} f : \mathbb{R}_+ &\longrightarrow \mathbb{Z} \\ x &\longmapsto \lfloor x \rfloor \end{aligned}$$

Cependant on ne peut pas toujours définir une application de cette manière.

Exemple. Posons $E = \{Pierre, Paul, Jack\}$. On peut alors définir une application de E dans $\mathbb{N}$ en associant son âge à chaque individus de E :

$$\begin{aligned} f : \{Pierre, Paul, Jack\} &\longrightarrow \mathbb{N} \\ Pierre &\longmapsto 21 \\ Paul &\longmapsto 30 \\ Jack &\longmapsto 25 \end{aligned}$$

Définition 1.1. Soient E, F, E' et F' des ensembles, f une application de E dans F et f' une application de E' da,s F'. Les applications f et f' sont dites *égales* si et seulement si on a $E = E'$, $F = F'$ et $f(x) = f'(x)$ pour tout x appartenant à E.

1 Composition

Définition 1.2. Pour tout ensemble E, l'application de E dans E qui à tout élément x de E associe x est *l'application identique de* E, on la note id_E.

Définition 1.3. Soient E, F et G des ensembles, f une application de E dans F et g une application de F dans G. L'application *composée* de f et g, notée $g \circ f$, est l'application

$$\begin{aligned} g \circ f : E &\longrightarrow G \\ x &\longmapsto g(f(x)) \end{aligned}$$

Le schéma suivant permet de mieux comprendre la définition :

$$\begin{aligned} g \circ f : E &\xrightarrow{f} \quad F \quad \xrightarrow{g} G \\ x &\longmapsto f(x) \longmapsto g(f(x)) \end{aligned}$$

Exemple.

– Pour tous ensembles E et F et pour toute application f de E dans E on a $f \circ \mathrm{id}_E = f$ et $\mathrm{id}_F \circ f = f$.

– Soient f l'application de $\mathbb{R}$ dans $\mathbb{R}$ qui à x associe $x + 1$ et g l'application de $\mathbb{R}$ dans $\mathbb{R}$ qui à x associe x^2. Alors on a

$$\begin{aligned} g \circ f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto (x+1)^2 \end{aligned}$$

– Soient f l'application de $E = \{Pierre, Paul, Jack\}$ dans $\mathbb{N}$ définit précédemment et g l'application de $\mathbb{N}$ dans $\mathbb{R}$ qui à tout x associe $\sqrt(x)$. Alors on a :

$$\begin{aligned} g \circ f : \{Pierre, Paul, Jack\} &\longrightarrow \mathbb{R} \\ Pierre &\longmapsto \sqrt{21} \\ Paul &\longmapsto \sqrt{30} \\ Jack &\longmapsto 5 \end{aligned}$$

Attention, en général, on a pas $f \circ g = g \circ f$. En effet pour $f : \mathbb{R} \to \mathbb{R}$ et $g : \mathbb{R} \to \mathbb{R}$ définies par $f(x) = x + 1$ et $g(x) = x^2$. On a

$$(g \circ f)(x) = (x+1)^2 = x^2 + 2x + 1 \neq (f \circ g)(x) = x^2 + 1.$$

Le résultat suivant montre que l'ordre dans lequel sont faites les compositions n'a pas d'importance.

Proposition 1.4. *Soient* E*,* F*,* G *et* H *des ensembles,* f *une application de* E *dans* F*,* g *une application de* F *dans* G *et* h *une application de* G *dans* H*. Alors on a* $h \circ (g \circ f) = (h \circ g) \circ f$.

Démonstration. Par définition de l'opération $\circ$, on a

$$\forall x \in E, (h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))),$$

ainsi que

$$\forall x \in E, ((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))).$$

Ces deux relations impliquent

$$\forall x \in E (h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x),$$

d'où $h \circ (g \circ f) = (h \circ g) \circ f$ par définition de l'égalité de fonctions. □

L'application $h \circ (g \circ f)$ est alors notée sans ambiguïté $h \circ g \circ f$.

2 Injection, surjection et bijection

Définition 1.5. On dit qu'une application $f : E \to F$ est *injective* ou que f est une *injection* si pour tout x et x' de E, on a l'implication $f(x) = f(x') \Rightarrow x = x'$.

Exemple. Les applications

$$\begin{array}{rcl} f : \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x+2 \end{array} \qquad \begin{array}{rcl} g : \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & e^x \end{array}$$

sont surjectives mais les applications

$$\begin{array}{rcl} h : \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2 \end{array} \qquad \begin{array}{rcl} i : \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \sin(x) \end{array}$$

ne le sont pas. En effet, on a $h(-1) = h(1) = 1$ et $i(0) = i(2\pi) = 0$.

Définition 1.6. On dit qu'une application $f : E \to F$ est *surjective*, ou que f est une *surjection*, si pour tout y de F, il existe x de E tel qu'on ait $f(x) = y$.

Exemple. Les applications

$$\begin{array}{rcl} f : \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x+2 \end{array} \qquad \begin{array}{rcl} g : \mathbb{R}_+^* & \to & \mathbb{R} \\ x & \mapsto & \log(x) \end{array}$$

sont surjective mais les applications

$$\begin{array}{rcl} h : \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & e^x \end{array} \quad \begin{array}{rcl} i : \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \sin(x) \end{array}$$

ne le sont pas. En effet -2 n'a pas d'antécédent par h ni par i.

Définition 1.7. On dit qu'une application $f : E \to F$ est *bijective*, ou que f et une *bijection*, si pour tout y de F, il existe un unique x de E tel qu'on ait $f(x) = y$.

Exemple. Les fonctions

$$\begin{array}{rcl} f : \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x+2 \end{array} \qquad \begin{array}{rcl} g : \mathbb{R}_+^* & \to & \mathbb{R} \\ x & \mapsto & \log(x) \end{array}$$

sont des bijections.

Attention, dire que la “fonction $\log$” est une une injection ou autre n'a pas de sens. Il est absolument nécessaire de préciser les ensembles de départ et d'arrivée.

Proposition 1.8. *Soient E et F deux ensembles et f une application de E dans F. L'application f est bijective si et seulement si elle est injective et surjective.*

Démonstration. Supposons que f soit bijective. Par définition, pour tout y de F il existe un unique x de E tel qu'on ait $f(x) = y$. En particulier un tel y existe et donc f est surjective. Soient x et x' deux élements de E tels qu'on ait $f(x) = f(x')$. Posons $y = f(x)$. L'application f étant bijective, il existe un unique x de E tel qu'on ait $f(x) = y$. La relation $f(x) = f(x') = y$ implique alors $x = x'$ et f est injective.

Supposons maitenenant que f est injective et surjective. Soit y un élément de F. Comme f est surjective, il existe x de E tel qu'on ait $f(x) = y$. Soit x' un élément de E vérifiant $f(x') = y$. L'application f étant injective, la relation $f(x) = y = f'x')$ implique nécaisserement $x = x'$. Il existe donc un unique élément x de E vérifiant $f(x) = y$. L'application f est donc bijective. $\square$

Proposition 1.9. *Soient E et F deux ensembles et f une application de E dans F. Alors f est bijective si et seulement s'il existe une application g de F dans E vérifiant $f \circ g = id_F$ et $g \circ f = id_E$. Si elle existe, l'application g est unique.*

Démonstration. Supposons que f soit bijective et montrons l'existence et l'unicité de g. Pour tout y de F, on note $g(y)$ l'unique x vérifiant $f(x) = y$. On a ainsi définit une application $g : F \to E$ vérifiant $f(g(y)) = y$, à savoir, $f \circ g = \mathrm{id}_F$. Montrons l'unicité de g. Supposons que h soit une fonction vérifiant aussi $f \circ h = \mathrm{id}_F$. Alors pour tout $y \in F$, on a $f(g(y)) = y = f(h(y))$, ce qui implique $g(y) = h(y)$ car f est bijective et donc injective. De la relation $f \circ g = \mathrm{id}_F$, on obtient $f(g(f(x))) = f(x)$ pour tout x de E. Puisque f est injective, on a $g(f(x)) = x$ pour tout x de E et donc $g \circ f = \mathrm{id}_E$.

Supposons maintenant que g existe et montrons que f est bijective. Soit y un élément de y. La relation $f \circ g = \mathrm{id}_F$ implique $f(g(y)) = y$. Il existe donc un élément x de E, à savoir $g(y)$, tel qu'on ait $f(x) = y$. L'application f est donc surjective. Soient x et x' deux élément de E vérifiant $f(x) = f(x')$. On a alors $g(f(x)) = g(f(x'))$. Ainsi, la relation $g \circ f = \mathrm{id}_E$ (vérifiée par hypothèses) implique

$$x = g(f(x)) = g(f(x')) = x',$$

ce qui montre que f est injective. Elle est donc bijective. □

L'application g est appelée *réciproque* de f et est notée f^{-1}.

Proposition 1.10. *Soient E et F deux ensembles et f une bijection de E dans F. alors f^{-1} est aussi une bijection et on a $(f^{-1})^{-1} = f$.*

Démonstration. Posons $g = f^{-1}$. Les relations $f \circ g = \mathrm{id}_F$ et $g \circ f = \mathrm{id}_E$ étant vérifiées, la proposition 1.9 assure que g est une bijection. Toujours grâce à la proposition 1.9, l'application f est unique, on a donc $g^{-1} = f$, à savoir $(f^{-1})^{-1} = f$. □

Proposition 1.11. *Soient E, F et G des ensembles et $f : E \to F$, $g : F \to G$ des bijections. L'application $g \circ f$ est alors bijective et l'on a $(g \circ f)^{-1} = f^{-1} \circ f^{-1}$.*

Démonstration. D'après la proposition 1.9, il existe des applications $f^{-1} : F \to E$ et $g^{-1} : G \to F$ telles que $f \circ f^{-1} = \mathrm{id}_F$, $f^{-1} \circ f = \mathrm{id}_E$, $g \circ g^{-1} = \mathrm{id}_G$ et $g^{-1} \circ g = \mathrm{id}_F$. Par associativité de $\circ$, on a

$$\begin{aligned}(g \circ f) \circ (f^{-1} \circ g^{-1}) &= ((g \circ f) \circ f^{-1}) \circ g^{-1} = ((g \circ (f \circ f^{-1}))) \circ g^{-1} \\ &= (g \circ \mathrm{id}_F) \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_G\end{aligned}$$

De même, on a

$$\begin{aligned}(f^{-1} \circ g^{-1}) \circ (g \circ f) &= ((f^{-1} \circ g^{-1}) \circ g) \circ f = ((f^{-1} \circ (g^{-1} \circ g)) \circ f \\ &= ((f^{-1} \circ \mathrm{id}_F) \circ f = f^{-1} \circ f = \mathrm{id}_E.\end{aligned}$$

L'application $g \circ f$ est donc bijective et on a $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

□

3 Lien avec les ensembles

Définition 1.12. Soit $f : E \to F$ une application
$i)$ Si A est une partie de E on appelle *image* de A par f et on note $f(A)$ l'ensemble

$$f(A) = \{y \in F \mid \exists x \in A, f(x) = y\}$$

$ii)$ Si B est une partie de F, on appelle *image réciproque* de B par f et on note $f^{-1}(B)$ l'ensemble

$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}$$

Attention, il ne faut pas confondre l'image réciproque d'un ensemble par f et la bijection réciproque f^{-1}, qui n'existe que si f est bijective.

Proposition 1.13. *Soit $f : E \to F$ une application.*
$i)$ *Pour toutes parties A, B de E, on a $f(A \cup B) = f(A) \cup f(B)$,$A \subset B \Rightarrow f(A) \subset f(B)$ et $f(A \cap B) \subset f(A) \cap f(B)$.*
$ii)$ *Pour toutes parties A, B de F, on a $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$, $A \subset B \Rightarrow f^{-1}(A) \subset f^{-1}(B)$ et $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.*

Démonstration. En TD $\square$

Définition 1.14. Un ensemble E est *fini* s'il existe est vide ou bien s'il existe un entier positif n et une bijection de E sur $\{1, \dots, n\}$.

Théorème 1.15. *Pour tout entiers positifs n et k. On a équivalence entre*
$i)$ $n \leqslant k$
$ii)$ *il existe une injection de $\{1, \dots, n\}$ dans $\{1, \dots, k\}$.*

Démonstration. Montrons que $i)$ implique $ii)$. On définit une application

$$\begin{aligned} f : \{1, \dots, n\} &\to \{1, \dots, k\} \\ i &\mapsto f(i) \end{aligned}$$

L'application f est bien définie car $n \geqslant k$ et c'est évidement une injection.

Montons maintenant $ii) \Rightarrow i)$. Soit f une injection de $\{1, \dots, n\}$ dans $\{1, \dots, k\}$. Pour tout entier n notons $\mathcal{P}_n$ la propriété : "s'il existe une injection de $\{1, \dots, n\}$ dans $\{1, \dots, n\}$, alors on a $n \leqslant k$". Montrons $\mathcal{P}_1$, pour qu'il existe une injection de $\{1\}$ dans $\{1, \dots, k\}$ il faut et il suffit qu'il existe une application de $\{1\}$ dans $\{1, \dots, k\}$ ce que revient à demander que l'ensemble $\{1, \dots, k\}$ soit non vide et donc $1 \geqslant k$.

Supposons $\mathcal{P}_{n-1}$ vraie et montrons $\mathcal{P}_n$ pour $n \geqslant 2$. Soient k un entier positif et f une injection de $\{1, \dots, n\}$ dans $\{1, \dots, k\}$. Pour pouvoir utiliser l'hypothèse de récurrence $\mathcal{P}_{n-1}$ nous allons, à partir de f, construire une application de $\{1, \dots, n-1\}$ dans $\{1, \dots, k-1\}$. Si k était égal à 1, on aurait $f(1) = f(n) = 1$ avec $n \neq 1$ ce qui est impossible car f est une injection. On en déduit $k \geqslant 2$. Plus généralement, pour tout $x \in \{1, \dots, n-1\}$, on a $f(x) \neq n$ car f est injective. Remarquons que $f(x) < f(n+1)$ implique $f(x) \leqslant f(n) - 1 \leqslant k - 1$ et donc $f(x) \in \{1, \dots, k-1\}$. Considérons l'application

$$\begin{aligned} g : \{1, \dots, n-1\} &\to \{1, \dots, k-1\} \\ x &\mapsto \begin{cases} f(x) & \text{si } f(x) < f(n) \\ f(x) - 1 & \text{si } f(x) > f(n) \end{cases} \end{aligned}$$

Supposons que g soit injective. Alors l'hypothèse de récurrence $\mathcal{P}_{n-1}$ implique $k-1 \leqslant n-1$ et donc $k \leqslant$n. Il nous reste donc à montrer que g est injective.

Soient x et y deux éléments de $\{1, \ldots, n\}$ tels qu'on ait $g(x) = g(y)$. On alors deux cas à traiter :

- si $f(x) < f(n)$ et $f(y) < f(n)$, il vient $g(x) = f(x)$ et $g(y) = f(y)$, d'où $f(x) = f(y)$ et donc $x = y$ (car f est injective).

- si $f(x) > f(n)$ et $f(y) > f(n)$, il vient $g(x) = f(x) - 1$ et $g(y) = f(y) - 1$, d'où $f(x) = f(y)$ et donc $x = y$.

Les cas $f(x) < f(n) < f(y)$ et $f(y) < f(n) < f(x)$ ne peuvent pas ce produire. Supposons $f(x) < f(n) < f(y)$. On aurait alos $g(x) = f(x)$ et $g(y) = f(y) - 1$, d'où $f(y) = f(x) + 1$ puis $f(x) < f(n) < f(x) + 1$. L'entier $f(n)$ serait donc compris entre deux entiers consécutifs, ce qui est impossible. De même pour $f(y) < f(n) < f(x)$. On a donc montré que g est injective, ce qui implique $n \leqslant k$. □

Corollaire 1.16. *Soit E un ensemble fini non vide. Il existe alors un unique entier positif n pour lequel il existe une bijection de E sur $\{1, \ldots, n\}$.*

Démonstration. Soient n et k deux entiers positifs et $f : E \to \{1, \ldots, n\}$ et $g : E \to \{1, \ldots, k\}$ des bijections. La composée de deux bijections étant une bijection, l'application $f \circ g^{-1}$ est une bijection (et donc une injection) de $\{1, \ldots, k\}$ sur $\{1, \ldots, n\}$ et l'application $g \circ f^{-1}$ est une bijection (et donc une injection) de $\{1, \ldots, n\}$ sur $\{1, \ldots, k\}$. On en déduit les inégalités $n \geqslant k$ et $k \neq n$ d'après le théorème 1.15. □

4 Cardinal d'un ensemble

Définition 1.17. Soit E un ensemble fini. Si E est vide, le *cardinal* de E est 0. Si E est non vide, le *cardinal* de E est l'unique entier n tel qu'il existe une bijection entre E et $\{1, \ldots, n\}$ Le cardinal de E se note $\operatorname{Card} E$ ou bien $\#E$.

Proposition 1.18. *Soient E et F des ensembles finis non vides. Il existe une bijection entre E et F si et seulement si on a* $\operatorname{Card} E = \operatorname{Card} F$.

Démonstration. Posons $n = \operatorname{Card} E$ et $k = \operatorname{Card} F$. Par définition du cardinal, il existe des bijection $g : E \to \{1, \ldots, n\}$ et $h : F \to \{1, \ldots, k\}$. Supposons qu'il existe une bijection f de E sur F. Alors l'application $h \circ f$ est une bijection de E dans $\{1, \ldots, k\}$ (par la proposition 1.11) et on a donc $k = n$ par le corollaire 1.16. Réciproquement, si n est égal à k, alors $h^{-1} \circ g$ est une bijection de E sur F. □

Proposition 1.19. *Tout sous-ensemble A d'un ensemble fini E est fini et on a* $\operatorname{Card}(A) \leqslant \operatorname{Card}(E)$.

Démonstration. Posons $n = \operatorname{Card}(E)$. Par définition du cardinal, il existe une bijection f de E sur l'ensemble $\{1, ..., n\}$. Soit A un sous ensembles de E. Notons g l'application de A dans $\{1, ..., n\}$ définie par $g(x) = f(x)$ pour $x \in A$. L'application g est injective. En effet la relation $g(x) = g(y)$ implique $f(x) = f(y)$ et donc $x = y$ car f est bijective et donc injective. Notons $i_1, ..., i_m$ avec $m \leqslant n$ et $i_1 < i_2 < ... < i_m$ les entiers de $\{1, ..., n\}$ appartenant réellement à $g(A)$ $(= f(A))$. On définit alors une application h de $g(A)$ dans $\{1, ..., m\}$, en posant $h(i_k) = k$. Par construction h est bijective. Comme g est injective de A dans $\{1, ..., n\}$, elle est bijective de A dans $g(A)$. L'application composée $(h \circ g)$ de A dans $\{1, ..., m\}$ est donc un bijection. Ce qui montre que A est un ensemble fini de cardinalité $\operatorname{Card}(A) = m \leqslant n = \operatorname{Card}(E)$. □

Proposition 1.20. *Soit E et F deux ensembles finis d'intersection vide. L'ensemble $E \cup F$ est alors fini et on a* $\mathrm{Card}(E \cup F) = \mathrm{Card}(E) + \mathrm{Card}(F)$.

Démonstration. Posons $n = \mathrm{Card}(E)$ et $m = \mathrm{Card}(F)$. Par définition du cardinal, il existe deux bijection $f : E \to \{1, ..., n\}$ et $g = F \to \{1, ..., m\}$. Notons h l'application de $E \cup F \to \{1, ..., n+m\}$ définie par

$$\begin{array}{rcl} h : E \cup F & \to & \{1, ..., n+m\} \\ x & \mapsto & \begin{cases} f(x) & \text{pour } x \in E, \\ n + g(x) & \text{pour } x \in F. \end{cases} \end{array}$$

Comme $E \cap F$ est vide, l'application h est bien définie (un seul des deux choix est possible). Montrons que h est une bijection. Commençons d'abord par montrer que c'est une surjection. Soit k un entier de $\{1, ..., n+m\}$. Si $k \leqslant n$, alors k appartient à un antécédent dans E par f et on a $h(f^{-1}(k)) = f(f^{-1}(k)) = k$, ce qui montre que k à aussi un antécédent par h. Si $k > n$, alors $k - n$ appratient à $\{0, ..., m\}$ qui possède un antécédent dans F par g. On a donc $h(g^{-1}(k-n)) = n + g(g^{-1}(k-n)) = n + k - n = k$. Ce qui montre que k a un antécédent par h et donc que h est surjective. Montrons maintenant que h est injective. Soient x et y deux éléments de $E \cup F$ tel que $h(x) = h(y)$. Si $h(x) \leqslant n$, les éléments x et y sont dans E et on a $f(x) = h(x) = h(y) = f(y)$ par définition de h, ce qui implique $x = y$ car f est une bijection et donc une injection. Si $h(x) > n$, les éléments x et y sont dans F et on a $g(x) = h(x) - n = h(y) - n = g(y)$ par définition de h, ce qui implique $x = y$ car g est une bijection et donc une injection.

On a donc montrer que g est une bijection et donc que $E \cup F$ est fini et qu'on a

$$\mathrm{Card}(E \cup F) = n + m = \mathrm{Card}(E) + \mathrm{Card}(F).$$

□

Proposition 1.21. *Soient E et F des ensemble finis non vides. Si $f : E \to F$ est une application , alors on a* $\mathrm{Card}\, f(E) \leqslant \mathrm{Card}\, E$. *De plus, on a* $\mathrm{Card}\, E = \mathrm{Card}\, F$ *si et seulement si l'application f est injective.*

Démonstration. Posons $n = \mathrm{Card}\, E$ et démontrons le résultat par récurrence sur n. Si $n = 1$, alors l'ensemble E a un seul élément et donc $f(E)$ aussi. Dans ce cas, on a $\mathrm{Card}\, f(E) = 1$ et f est injective. Supposons le résultat vrai pour $n - 1$ et montrons le pour n avec $n \geqslant 2$. Soit a un élément de E et posons $E' = E \setminus \{a\}$. On a donc $\mathrm{Card}\, E' = n - 1$ Soit g l'application définie par

$$\begin{array}{rcl} g : E' & \to & F \\ x & \mapsto & f(x) \end{array}$$

On a $f(E) = g(E') \cup \{f(a)\}$ et donc, par la proposition 1.20

$$\mathrm{Card}\, f(E) = \begin{cases} \mathrm{Card}\, g(E') + 1 & \text{pour } f(a) \notin g(E') \\ \mathrm{Card}\, g(E') & \text{pour } f(a) \in g(E'). \end{cases}$$

Par hypothèse de récurrence, on a $\mathrm{Card}\, g(E') \leqslant \mathrm{Card}\, E' = n - 1$ et donc $\mathrm{Card}\, f(E) \leqslant n = \mathrm{Card}\, E$. De plus f est injective si et seulement si g l'est et $f(a)$ n'est pas un élément de $g(E')$, ce qui par hypothèse de récurrence revient à $\mathrm{Card}\, g(E) = n - 1$ et $f(a) \notin g(E')$, qui est encore équivalent à $\mathrm{Card}\, f(E) = \mathrm{Card}\, E$. □

Corollaire 1.22. *Tout sous-ensemble A d'un ensemble fini E est fini et on a* $\mathrm{Card}(A) \leqslant \mathrm{Card}(E)$. *De plus A est égal à E si et seulement si* $\mathrm{Card}(A) = \mathrm{Card}(E)$.

Démonstration. Si A est l'ensemble vide alors A est fini et on $0 = \mathrm{Card}(A) \leqslant \mathrm{Card}(E)$ avec égalité si et seulement si $E = \emptyset = A$. Supposons maintenant que A est non vide. Soit a un élément de A. On définit alors une application f de E dans A en posant

$$\begin{aligned} f : E &\to A \\ x &\mapsto \begin{cases} x & \text{si } x \in A \\ a & \text{si } x \in E \setminus A \end{cases} \end{aligned}$$

Par construction de f, on a $f(E) = A$. La proposition 1.21 garantit alors que $A = f(E)$ est finie ainsi que $\mathrm{Card}(A) = \mathrm{Card}(f(E)) \leqslant \mathrm{Card}(E)$. Toujours par la proposition 1.21, on a $\mathrm{Card}(A) = \mathrm{Card}(E)$ si et seulement si f est injective. Or si $E \setminus A$ est non vide, il contient un élément x n'appartenant pas à A et on a $f(x) = f(a) = a$. Ainsi f est injective si et seulement si $E \setminus A = \emptyset$ et donc si et seulement si $A = E$. $\square$

Proposition 1.23 (Principe des tiroirs)**.** *Soient E, F des ensembles finis non vides et $f : E \to F$ une application. Si* $\mathrm{Card}\, E > \mathrm{Card}\, F$ *alors il existe $x, y \in E$ avec $x \neq y$ et $f(x) = f(y)$.*

Démonstration. Puisque $f(E)$ est inclus dans F, on a $\mathrm{Card}(f(E)) \leqslant \mathrm{Card}\, F < \mathrm{Card}\, E$. Ainsi, par la proposition 1.21 f n'est pas injective. Il existe donc x et y dans E avec $x \neq y$ et $f(x) = f(y)$. $\square$

Théorème 1.24. *Soient E, F des ensembles finis non vides et $f : E \to F$ une application. Si* $\mathrm{Card}\, E = \mathrm{Card}\, F$*, alors les propriétés suivantes sont équivalentes :*
$i)$ *f est bijective,*
$ii)$ *f est injective,*
$iii)$ *f est surjective.*

Démonstration. On a évidement $i) \Rightarrow ii)$, $i) \Rightarrow iii)$ et $(\ ii)\,\text{et}\,iii)\ ) \Rightarrow i)$. Il suffit alors de montrer $ii) \Leftrightarrow iii)$. L'application f est surjective si et seulement si $f(E) = F$, donc si et seulement si $\mathrm{Card}\, f(E) = \mathrm{Card}\, F$. Or, par hypothèse, on a $\mathrm{Card}\, E = \mathrm{Card}\, F$. Ainsi f est surjective si et seulement si on a $\mathrm{Card}\, f(E) = E$ et donc si et seulement si f est injective d'après la proposition 1.21. $\square$

5 Cardinal et opérations d'ensembles

Proposition 1.25. *Soient E et F des ensembles finis, alors $E \cup F$ est fini et* $\mathrm{Card}(E \cup F) = \mathrm{Card}(E) + \mathrm{Card}(F) - \mathrm{Card}(E \cap F)$.

Démonstration. Posons $G = E \setminus F$. On a $E \cup F = G \cup F$. Comme G est fini comme sous-ensemble d'un ensemble fini. De plus l'intersection $G \cap F$ est vide. L'ensemble $G \cup F$ est donc fini, ce qui par la proposition 1.20 donne

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

Par ailleurs, on a $E = (E \setminus F) \cup (E \cap F)$ ainsi que $(E \setminus F) \cap (E \cap F) = \emptyset$. On a donc, toujours a proposition 1.20,

$$\mathrm{Card}(E) = \mathrm{Card}(E \setminus F) + \mathrm{Card}(E \cap F) = \mathrm{Card}(G) + \mathrm{Card}(E \cap F).$$

D'où $\mathrm{Card}(G) = \mathrm{Card}(E) - \mathrm{Card}(E \cap F)$ puis

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

□

Définition 1.26. Soient $E_1, ..., E_n$ des ensembles. Ont dit que ces ensembles sont disjoints 2 à 2 si pour tout i, j de $\{1, ..., n\}$ avec $i \neq j$, on a $E_i \cap E_j = \emptyset$.

Définition 1.27. La réunion d'ensembles $E_1, ..., E_n$ est définie par

$$\bigcup_{i=1}^{n} E_i = (...(E_1 \cup E_2) \cup ...) \cup E_n)$$

Si de plus les E_i sont deux à deux disjoints, leur réunion est notée $\displaystyle\bigsqcup_{i=1}^{n} E_i$.

Proposition 1.28. *Soient $E_1, ..., E_n$ des ensembles disjoints deux à deux, alors on a*

$$\mathrm{Card}\left(\bigsqcup_{i=1}^{n} E_i\right) = \sum_{i=1}^{n} \mathrm{Card}(E_i).$$

Démonstration. Par récurrence sur n. Pour $n = 1$, il n'y a rien à montrer. Pour $n = 2$ c'est la proposition 1.20. Supposons le résultat vrai pour $n - 1$ et montrons le pour $n1$. Soient $E_1, ..., E_{n-1}, E_n$ des ensembles disjoints 2 à 2. Par hypothèse de récurrence, on a

$$\mathrm{Card}\left(\bigsqcup_{i=1}^{n-1} E_i\right) = \sum_{i=1}^{n-1} \mathrm{Card}(E_i).$$

Posons $F = \bigsqcup_{i=1}^{n-1} E_i$ et montrons que l'intersection $F \cap E_n$ est vide. Supposons par l'absurde que x soit un élément de $F \cap E_n$. Comme x appartient à F, il existe $i \in \{1, ..., n-1\}$ tel que x appartienne à E_i. On a donc $x \in E_i \cap E_n$, ce qui contredit que les E_i sont disjoints 2 à 2. On a donc bine $F \cap E = \emptyset$. Ainsi, en appliquant la proposition 1.20, on obtient $\mathrm{Card}(F \cup E_n) = \mathrm{Card}(F) + \mathrm{Card}(E_n)$ et donc

$$\mathrm{Card}\left(\bigsqcup_{i=1}^{n} E_i\right) = \mathrm{Card}(F \cup E_n) = \left(\sum_{i=1}^{n-1} \mathrm{Card}(E_i)\right) + \mathrm{Card}(E_n) = \sum_{i=1}^{n} \mathrm{Card}(E_i).$$

□

Définition 1.29. Si E et F sont des ensembles, le *produit cartésien* de E par F, noté $E \times F$, est l'ensemble *couples* (x, y), où x décrit E et où y décrit F. Les couples (x, y) et (x', y') sont égaux si et seulement si on a $x = x'$ et $y = y'$.

Si E est un ensemble, le produit cartésien $E \times E$ se note E^2. Par exemple, le produit cartésien $\mathbb{R}^2$ est formé des couples de nombres réels ; ceux-ci permettent de déterminer un point du plan par ses coordonnées, lorsqu'on s'est donné un repère cartésien.

Plus généralement, pour tout entier n supérieur ou égal à 2, le produit cartésien de E par lui-même n fois se note E^n. Les éléments de E^n sont les *n-uplets* $(x_1, x_2, ..., x_n)$, où les éléments $x_1, x_2, ..., x_n$ appartiennent à E. Les n-uplets $(x_1, x_2, ..., x_n)$ et $(y_1, y_2, ..., y_n)$ sont égaux si et seulement si on a $x_i = y - i$ pour tout $i = 1, 2, ..., n$.

Proposition 1.30. *Si E et F sont des ensembles finis, le produit cartésien $E \times F$ est un ensemble fini et l'on a* $\mathrm{Card}(E \times F) = \mathrm{Card}(E) \times \mathrm{Card}(F)$.

Démonstration. L'ensemble $E \times F$ est l'ensemble des couples (x, y) avec $x \in E$ et $y \in F$. Pour x dans E, on note F_x l'ensemble des couples (x, y) avec y décrivant F. Les ensembles F_x étant deux à deux disjoints on a

$$E \times F = \bigsqcup_{x \in E} F_x$$

L'application f_x de F_x dans F défini par $f_x(x, y) = y$ étant une bijection de F_x sur F, on a $\mathrm{Card}\, F_x = \mathrm{Card}(F)$. Ce qui, par la proposition 1.28 donne

$$\mathrm{Card}(E \times F) = \mathrm{Card}\left(\bigsqcup_{x \in E} F_x\right) = \sum_{x \in E} \mathrm{Card}(F_x) = \sum_{x \in E} \mathrm{Card}(F) = \mathrm{Card}(E) \times \mathrm{Card}(F)$$

□

Proposition 1.31. *Si E et F sont des ensembles finis non vides, alors il y'a* $\mathrm{Card}(F)^{\mathrm{Card}(E)}$ *applications de E dans F.*

Démonstration. Posons $n = \mathrm{Card}(E)$, $k = \mathrm{Card}(F)$ et démontrons le résultat par récurrence sur n. Si l'ensemble E n'a qu'un élément, c'est-à-dire $n = 1$, alors le nombre d'applications de E dans F est le nombre d'images possibles pour cet élément, c'est à dire k. Supposons $n \geqslant 2$ et la propriétés démontrée pour un ensemble de départ de cardinal $n - 1$. Choisissons $a \in E$ et posons $E' = E \setminus \{a\}$. Il vient $\mathrm{Card}(E') = n - 1$. Par hypothèse de récurrence il y'a k^{n-1} applications de E' dans F. Pour tout y de F il y'a donc k^{n-1} applications de E dans F envoyant a sur y. On en déduit qu'il y'a $k \times k^{n-1}$ applications de de E dans F. □

En particulier, si E à n éléments il y'a n^n applications de E dans E. Ainsi il y'a 3125 applications de $1, 2, 3, 4, 5$ dans lui même.

Proposition 1.32. *Si E et F sont des ensembles de cardinal n, alors il y'a $n!$ bijections de E sur F.*

Démonstration. On démontre le résultat par récurrence sur n. Si $n = 1$ il y'a une seule application de E dans F qui est forcément bijective. Supposons $n \geqslant 2$ et le résultat démontré pour des ensembles de cardinal $n - 1$. Choisissons un élément a de E. Pour tout $y \in F$, on a $\mathrm{Card}(E \setminus \{a\}) = \mathrm{Card}(F \setminus \{y\}) = n - 1$. Par hypothèse de récurrence il y'a donc $(n - 1)!$ bijections de $E \setminus \{a\}$ dans $F \setminus \{y\}$. On en déduit que pour tout $y \in F$, il y'a $(n - 1)!$ bijections f de E sur F envoyant a sur y. Il y'a donc $n \times (n - 1)!$ bijections de E sur F. □

En particulier, sur les 3125 applications de $\{1, 2, 3, 4, 5\}$ dans lui-même seulement 120 sont des bijections.

Proposition 1.33. *Si E est un ensemble fini non vide, alors il y a* $2^{\mathrm{Card}(E)}$ *parties de E.*

Démonstration. Soit A un sous ensemble de E. On définie l'application χ_A de E dans $\{0, 1\}$ par

$$\begin{aligned} \chi_A : E &\to \{0, 1\} \\ x &\mapsto \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \in E \setminus A \end{cases} \end{aligned}$$

Notons F l'ensemble des applications de E dans $\{0,1\}$. On définit alors une application χ de $P(E)$ dans F qui envoie toute partie A de E sur χ_A. Montrons que l'application χ est bijective. Soit ϕ une application de E dans $\{0,1\}$. La fonction χ envoie alors $\phi^{-1}\{1\}$ sur $\chi_{\phi^{-1}\{1\}}$ avec $\chi_{\phi^{-1}\{1\}}(x) = 1$ si et seulement si $x \in \phi^{-1}(1)$ et donc si et seulement si $\phi(x) = 1$. On a donc $\chi_{\phi^{-1}\{1\}} = \phi$ et χ est surjective. Montrons que χ est injective. Soient A et B deux élément de $P(E)$ tels que $\chi(A) = \chi_A = \chi_B = \chi(B)$. On a a donc

$$x \in A \Leftrightarrow \chi_A(x) = 1 \Leftrightarrow \chi_B(x) = 1 \Leftrightarrow x \in B,$$

ce qui montre $A = B$. L'application χ étant bijective, on a $\mathrm{Card}(P(E)) = \mathrm{Card}(F) = 2^{\mathrm{Card}(E)}$ par la proposition 1.31. $\square$

II. Relations

Dans tous ce chapitre E désigne un ensemble quelconque, fini ou pas.

1 Généralités

Définition 2.1. Une *relation binaire* $\mathcal{R}$ sur E est une propriété que chaque couple (x, y) de $E \times E$ est susceptible de vérifier ou non. Si le couple vérifie la relation $\mathcal{R}$, on note $x\mathcal{R}y$.

Exemple. Sur $\mathbb{R}$, vous connaissez déjà les relations $=$, $\neq$, $<$, $>$, $\leqslant$, $\geqslant$ ... . Sur $\mathbb{Z}$, "x divise y" est une relation binaire.

Définition 2.2. Deux relations binaires $\mathcal{R}$ et $\mathcal{R}'$ sur E sont égales si

$$\forall (x, y) \in E \times E, \quad x\mathcal{R}y \Leftrightarrow x\mathcal{R}'y$$

Proposition 2.3. *Soit* $\mathrm{Rel}(E)$ *l'ensemble des relations binaires sur* E*. L'application*

$$\begin{array}{rcl} \mathcal{G} : \mathrm{Rel}(E) & \to & \mathcal{P}(E \times E) \\ \mathcal{R} & \mapsto & \{(x, y) \in E \times E \,|\, x\mathcal{R}y\} \end{array}$$

est une bijection.

Démonstration. Montrons d'abord que $\mathcal{G}$ est une surjection. Soit F une partie de $E \times E$ alors la relation $\mathcal{R}_F$ définie par $x\mathcal{R}_F y$ si et seulement si (x, y) appartient à F vérifie

$$\mathcal{G}(\mathcal{R}_F) = \{(x, y) \in E \times E \,|\, x\mathcal{R}_F y\} = \{(x, y) \in E \times E \,|\, (x, y) \in F\} = F.$$

Montrons que $\mathcal{G}$ est injective. Soient $\mathcal{R}$ et $\mathcal{R}'$ deux relations binaires sur E vérifiant $\mathcal{G}(\mathcal{R}) = \mathcal{G}(\mathcal{R}')$. On a

$$\begin{aligned} \mathcal{G}(\mathcal{R}) = \mathcal{G}(\mathcal{R}') &\Rightarrow \{(x, y) \in E \times E \,|\, x\mathcal{R}y\} = \{(x, y) \in E \times E \,|\, x\mathcal{R}'y\} \\ &\Rightarrow \forall (x, y) \in E \times E, \quad x\mathcal{R}y \Leftrightarrow x\mathcal{R}'y \\ &\Rightarrow \mathcal{R} = \mathcal{R}' \end{aligned}$$

La fonction $\mathcal{G}$ est alors injective et surjective donc bijective. $\square$

Ce donner une relation sur E revient donc à se donner une partie de $E \times E$.

Définition 2.4. Soit $\mathcal{G}$ l'application définit précédemment. Alors pour toute application binaire $\mathcal{R}$ de E, la partie $\mathcal{G}(\mathcal{R})$ de $E \times E$ est appelé *graphe* de la relation $\mathcal{R}$.

Exemple. Le graphe de la relation $=$ sur $\mathbb{R}$ est faire dessin Le graphe de la relation $\leqslant$ sur $\mathbb{R}$ est faire dessin

Définition 2.5. Soit $\mathcal{R}$ une relation binaire sur un ensemble E. On dit que

- $\mathcal{R}$ est *réflexive* si : $\forall x \in E,\ x\mathcal{R}x$;
- $\mathcal{R}$ est *symétrique* si : $\forall x, y \in E,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x$;
- $\mathcal{R}$ est *transitive* si : $\forall x, y, z \in E,\ x\mathcal{R}y \,\text{et}\, y\mathcal{R}z \Rightarrow x\mathcal{R}z$;
- $\mathcal{R}$ est *antisymétrique* si : $\forall x, y \in E,\ x\mathcal{R}y \,\text{et}\, y\mathcal{R}x \Rightarrow x = y$.

Exemple. Parmi les relations $=$, $\neq$, $<$, $>$,$\leqslant$, $\geqslant$ de $\mathbb{R}$ seules les relations Sur $\mathbb{R}$ les relations
- $=$, $\leqslant$ et $\geqslant$ sont réfléxives ;
- $=$, $\neq$ sont symétriques ;
- $=$, $<$, $>$, $\leqslant$, $\geqslant$ sont transitives ;
- $=$, $\leqslant$, $\geqslant$ sont antisymétriques.

2 Relation d'ordre

Définition 2.6. Une relation binaire $\mathcal{R}$ sur E est une *relation d'ordre au sens large* si c'est une relation réflexive, transitive et antisymétrique.

Exemple. Sur $\mathbb{R}$ les relations $=$, $\leqslant$ et $\geqslant$ sont des relations d'ordre aux sens large mais pas $\neq$, $<$ et $>$. Sur $\mathbb{N}$ la relation de divisibilité est une relation d'ordre au sens large, mais c'est ce n'est par une relation d'ordre sur $\mathbb{Z}$: elle n'est pas antisymétrique -1 divise 1 et 1 divise -1 sans qu'on est $-1 = 1$.

Définition 2.7. Une relation binaire $\mathcal{R}$ sur E est une *relation d'ordre au sens strict* si c'est une relation non réflexive, transitive et antisymétrique.

Exemple. Sur $\mathbb{R}$ les relations $<$ et $>$ sont des relations d'ordre au sens strict mais pas $=$, $\neq$, $\leqslant$ et $\geqslant$. Sur $\mathbb{N}$, la relation de divisibilité n'est pas une relation d'ordre au sens strict.

Définition 2.8. Une relation d'ordre au sens large $\mathcal{R}$ sur E est dite *totale* si pour tout éléments x, y de E on a $x\mathcal{R}y$ ou $y\mathcal{R}x$. Une relation d'ordre au sens stricte $\mathcal{R}$ sur E est dite *totale* si pour tout éléments x, y de E on a $x = y$ ou $x\mathcal{R}y$ ou $y\mathcal{R}x$. Une relation d'ordre qui n'est pas totale est dite *partielle*.

Exemple. Sur $\mathbb{R}$, les relations $=$,$<$,$>$,$\leqslant$,$\geqslant$ sont totales. Par contre la relation de divisibilité est une relation d'ordre partielle sur $\mathbb{N}$. On a pas 2 divise 3 ni 3 divise 2. Les éléments 2 et 3 ne sont donc pas comparables vis à vis de la relation de divisibilité.

3 Relation d'équivalence

Définition 2.9. Une relation binaire $\mathcal{R}$ sur E est une relation d'*équivalence* si c'est une relation réflexive, symétrique et transitive.

Exemple. Soit $n \in \mathbb{N}$. Pour tout $a, b \in \mathbb{Z}$, on pose $a \equiv b \mod n$ ou encore $a \equiv_n b$ si n divise $b - a$. C'est la *congruence modulo* n. La relation $\equiv_n$ est une relation d'équivalence sur $\mathbb{Z}$:
- elle est réflexive : soit $a \in \mathbb{Z}$. Comme $0 = a - a$ est divisible par n, on a $a \equiv_n a$.
- elle est symétrique : soient $a, b \in \mathbb{Z}$ tels que $a \equiv_n b$. Il existe alors $k \in \mathbb{Z}$ tel que $b - a = kn$. On a donc $a - b = (-k)n$ et donc $b \equiv_n b$.
- elle est transitive : soient a, b, c de $\mathbb{Z}$ tels que $a \equiv_n b$ et $b \equiv_n c$. Il existe alors $k, l \in \mathbb{Z}$ tel que $b - a = kn$ et $c - b = ln$. On a donc $c - a = (c - b) + (b - a) = ln + kn = (l + k)n$ puis $a \equiv_n c$.

Définition 2.10. Soit $\mathcal{R}$ une relation d'équivalence sur E. Une *classe d'équivalence* de E pour $\mathcal{R}$ est l'ensemble

$$F = \{y \in E \mid x\mathcal{R}y\} \quad \text{où } x \text{ est fixé}$$

On note $F = [x]_{\mathcal{R}}$. On dit que F est la classe d'équivalence de x et que x est un représentant de F. Quand le contexte est assez clair, on note $[x]$ à la place de $[x]_{\mathcal{R}}$.

Exemple. Considérons la congruence modulo 2 sur $\mathbb{N}$. La classe d'équivalence de 2 est

$$[2] = \{0, 2, 4, 6, 8, 10, 12, ...\}$$

l'ensemble des nombres pairs. La classe de $[3]$ est l'ensemble des nombres impairs. Remarquons l'égalité $[2] = [4]$.

Définition 2.11. On dit que $\{F_1, ..., F_n\}$ est une partition de E si on a $\bigcup_{i=1}^n F_i = E$ et si pour tout $i \neq j$ on a $F_i \cap F_j = \emptyset$. Ce qu'on note

$$E = \bigsqcup_{i=1}^{n} F_i$$

Théorème 2.12. *Soit $\mathcal{R}$ une relation d'équivalence sur E. Alors les classes d'équivalences de E pour $\mathcal{R}$ forment une partition de E.*

Démonstration. Notons $\mathcal{C}_{\mathcal{R}}$ l'ensemble des classes d'équivalences de $\mathcal{R}$. Choisissons dane chaque classe d'équivalence un unique représentant de manière à obtenir un sous ensemble $\mathcal{E}_{\mathcal{R}}$ vérifiant

$$\{[x] \mid x \in \mathcal{E}_{\mathcal{R}}\} = \mathcal{C}_{\mathcal{R}}$$

Montrons $E = \bigcup_{x \in \mathcal{C}_{\mathcal{R}}} [x]$. Soit $y \in E$. L'ensemble $F = \{z \in E \mid y\mathcal{R}z\}$ est une classe d'équivalence de $\mathcal{R}$. Par construction de $\mathcal{E}_{\mathcal{R}}$, il existe $x \in \mathcal{E}_{\mathcal{R}}$ avec $y \in [x]$. On a donc

$$y \in \bigcup_{x \in \mathcal{E}_{\mathcal{R}}} [x]$$

puis $E \subseteq \bigcup_{x \in \mathcal{E}_{\mathcal{R}}} [x]$. L'inclusion dans l'autre sens est évidente car $[x] \subseteq E$ pour tout $x \in \mathcal{E}_{\mathcal{R}}$

Montrons maintenant que les classes $[x]$ avec $x \in \mathcal{E}_{\mathcal{R}}$ sont deux à deux distinctes. Soient $x, y \in \mathcal{E}_{\mathcal{R}}$ avec $x \neq y$. Par l'absurde, on suppose $[x] \cap [y] \neq \emptyset$. Il existe alors $z \in [x] \cap [y]$, d'où $x\mathcal{R}z$ et $y\mathcal{R}z$. Par symétrie de $\mathcal{R}$, on a $z\mathcal{R}y$. Puis $x\mathcal{R}y$ par transitivité de $\mathcal{R}$. On a donc $y \in [x]$. De manière similaire, on montre $x \in [y]$. On obtient alors $[x] = [y]$, ce qui, par construction de $\mathcal{E}_{\mathcal{R}}$ donne $x = y$. Contradiction. □

Remarque : L'ensemble des classes d'équivalences $\mathcal{C}_{\mathcal{R}}$ est appelé *ensemble quotient* de E par $\mathcal{R}$. Le décrire revient souvent à construire un bon ensemble de représentants $\mathcal{E}_{\mathcal{R}}$.

Exemple. Congruence modulo 5 sur $\mathbb{Z}$ a pour classes d'équivalence

$$\begin{aligned}
[0] &= \{..., -10, -5, 0, 5, 10, ...\} = \{5k \mid k \in \mathbb{Z}\} \\
[1] &= \{..., -9, -4, 1, 6, 11, ...\} = \{5k + 1 \mid k \in \mathbb{Z}\} \\
[2] &= \{..., -8, -3, 2, 7, 12, ...\} = \{5k + 2 \mid k \in \mathbb{Z}\} \\
[3] &= \{..., -7, -2, 3, 8, 13, ...\} = \{5k + 3 \mid k \in \mathbb{Z}\} \\
[4] &= \{..., -6, -1, 4, 9, 14, ...\} = \{5k + 4, \mid k \in \mathbb{Z}\}
\end{aligned}$$

où $\mathcal{E}_{\mathcal{R}} = \{0, 1, 2, 3, 4\}$. On note $\mathcal{C}_{\mathcal{R}}$ par $\mathbb{Z}/5\mathbb{Z}$. On identifie souvent $\mathbb{Z}/5\mathbb{Z}$ avec l'ensemble naturel de représentants $\mathcal{E}_{\mathcal{R}} = \{0, 1, 2, 3, 4\}$.

Définition 2.13. Soit $\mathcal{R}$ une relation d'équivalence sur E. L'ensemble des classes d'équivalences de E pour $\mathcal{R}$ est appelé *ensemble quotient* de E par $\mathcal{R}$ et se note $E\mathcal{R}$.

Exemple. La relation $\equiv_n$ est une relation d'équivalence sur $\mathbb{Z}$. L'ensemble quotient de $\mathbb{Z}$ par $\equiv_n$ est

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\equiv_n = \{[0], [1], ..., [n-1]\}.$$

III. Système linéaire

1 Définitions de base

Définition 3.1. Une équation linéaire à n variables $x_1, x_2, ..., x_n$ dans un corps k ($\mathbb{R}$ ou $\mathbb{C}$) est une équation de la forme

$$a_1x_1 + a_2x_2 + ... + a_nx_n = b$$

où $a_1, a_2, ..., a_n$ sont des éléments de k.

Exemple. Dans le plan $\mathbb{R}^2$, une équation linéaire $ax + by = c$ définit une droite. Dans l'espace $\mathbb{R}^3$, une équation linéaire $ax + by + cz = d$ définit un plan.

Définition 3.2. Un système d'équations linéaires à n variables est de la forme :

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + ... + a_{1,n}x_n = b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + ... + a_{2,n}x_n = b_2 \\ ... \\ a_{m,1}x_1 + a_{m,2}x_2 + ... + a_{m,n}x_n = b_m \end{cases}$$

Par convention : $a_{i,j}$ désigne le coefficient de x_j dans la i-ème équation.

Principe de résolution d'un système linéaire :

$$\begin{array}{ccc} \text{système linéaire} & \rightarrow & \text{matrice (tableau de nombres)} \\ & & \downarrow \\ \text{solution} & \leftarrow & \text{matrice simplifiée} \end{array}$$

Définition 3.3. Un vectuer $\vec{u}$ de k^n est une colonne de n éléments de k

$$\vec{u} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad \text{avec } x_i \in k \text{ pour } i = 1, ..., n.$$

Définition 3.4. Une matrice de taille $m \times n$ sur k est un tableau à m lignes et n colonnes d'éléments de k

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & ... & a_{1,n} \\ a_{2,1} & a_{2,2} & ... & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & ... & a_{n,n} \end{bmatrix} \quad \text{avec } a_{i,j} \in k \text{ pour } i = 1, ..., m \text{ et } j = 1, ..., n$$

Par convention les *coefficients* d'une matrice A sont notés $a_{i,j}$ où i désigne le numéro de ligne et j le numéro de colonne.

Exemple.

$$\begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix} \quad \text{est un vecteur de } \mathbb{R}^3 \qquad et \qquad \begin{bmatrix} 1 & 0 \\ 0 & -1 \\ 2 & 3 \end{bmatrix} \quad \text{est une matrice } 3 \times 2 \text{ sur } \mathbb{R}.$$

Définition 3.5. Le prouduit d'une matrice A de taille $m \times n$ et d'un vecteur de taille n est

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{1,1}x_1 + a_{1,2}x_2 + \dots + a_{1,n}x_n \\ a_{2,1}x_1 + a_{2,2}x_2 + \dots + a_{2,n}x_n \\ \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \dots + a_{m,n}x_n \end{bmatrix}$$

Exemple.

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & -1 \end{bmatrix}$$

Pour avoir un produit $A \cdot \vec{u}$ il faut que le nombre de colonne de A soit égal à la taille de $\vec{u}$.

Un système linéaire à m équations et n indeterminées s'écrit $A \cdot \vec{x} = \vec{b}$ où
- A est la matrice $m \times n$ des coefficients
- le vecteur $\vec{b}$ de taille m est le terme constant
- le vecteur $\vec{x}$ de taille n est celui des indéterminées

Exemple. Pour le système

$$S = \begin{cases} x_1 - x_2 + x_3 & = 1 \\ x_1 - x_3 & = 2 \end{cases}$$

on a

$$A = \begin{bmatrix} 1 & -1 & 1 \\ 1 & 0 & -1 \end{bmatrix}, \qquad \vec{b} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad \vec{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}.$$

Le système S sécrit donc

$$\begin{bmatrix} 1 & -1 & 1 \\ 1 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$$

Définition 3.6. La matrice *augmentée* d'un système linéaire $A \cdot \vec{x} = \vec{b}$ à m équations et n indeterminées est une matrice de taille $m \times (n+1)$

$$\left[\begin{array}{c|c} A & \vec{b} \end{array} \right]$$

Exemple. La matrice augmentée de

$$S = \begin{cases} x_1 - x_2 + x_3 & = 1 \\ x_1 - x_3 & = 2 \end{cases} \quad \text{est} \quad \left[\begin{array}{ccc|c} 1 & -1 & 1 & 1 \\ 1 & 0 & -1 & 2 \end{array} \right]$$

On aimerait simplifier la matrice augmentée d'un système S sans modifier l'ensemble des solutions du système.

Définition 3.7. Deux systèmes linéaires de m équations et n indeterminées S, S' sont *équivalents* s'ils ont exactement le même ensemble de solution.

Définition 3.8. Soit M une matrice. Les *opérations élémentaires sur les lignes* sont

$i)$ Echanger deux lignes noté $L_i \leftrightarrow L_j$

$ii)$ Multiplier une ligne par une constante $c \neq 0$, noté $L_i \leftarrow cL_i$

$iii)$ Ajouter à une ligne c fois une autre, noté $L_i \leftarrow L_i + cL_j$

Proposition 3.9. *Soient S, S' des systèmes linéaires et M, M' leurs matrices augmentées respectives. Si M' est obtenu de M à l'aide d'une opération élémentaire sur les lignes alors les système S et S' sont équivalents.*

Démonstration. $i)$ Echanger deux lignes correspond à échanger les deux équations correpsondantes : les solutions du système restent les mêmes

$ii)$ $\vec{x}$ est solution de l'équation définie par L_i

$\Leftrightarrow m_{i,1}x_1 + m_{i,2}x_2 + ... + m_{i,n}x_n = m_{i,n+1}$

$\Leftrightarrow cm_{i,1}x_1 + cm_{i,2}x_2 + ... + cm_{i,n}x_n = cm_{i,n+1}$

$\Leftrightarrow$ $\vec{x}$ est solution de l'équation définie par L'_i.

Les autres lignes L'_j avec $j \neq i$ sont identiques aux L_j. S est donc équivalent à S'.

$iii)$ Supposons que la ligne L'_i de M' soit donnée par $L'_i = L_i + cL_j$.

Montrons que si $\vec{x}$ est solution de S alors $\vec{x}$ est solution de S'. Supposons que $\vec{x}$ soit solution de L_i et L_j. Il est alors solution de L_i et cL_j et donc solution de $L_i + cL_j$ à savoir L'_i. Commes les autres lignes se M' sont identiques à celles de M, $\vec{x}$ est solution de S'.

Montrons maintenant que si $\vec{x}$ est solution de S', alors il est solution de S. On a $L'_i = L_i + cL_j$ et donc $L_i = L'_i - cL_j = L'_i - cL'_j$. Supposons que $\vec{x}$ soit solution de L'_i et L'_j. Il est alors solutiond de L'_i et cL'_j et donc solution de $L'_i + cL'_j = L_i$. Commes les autres lignes se M sont identiques à celles de M', $\vec{x}$ est solution de S. □

2 Méthode du pivot de Gauß

Définition 3.10. Une matrice A est *échelonée réduite* si :

$i)$ les r premières lignes sont non-nulles, et les $m - r$ dernières lignes sont nulles

$ii)$ le premier élement des lignes non nulles est 1

$iii)$ si on note par $p(i)$ la position du premier élément non nul de L_i, on a $p(1) < p(2) < ... < p(r)$ où r est la position de la dernière ligne non nulle

$iv)$ les colonnes $C_{p(1)}, C_{p(2)}, ..., C_{p(r)}$ sont de la forme

$$\begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Exemple.

$$\left[\begin{array}{c|c|cc|c|ccc} 0 & 1 & 3 & 5 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 4 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 3 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

Théorème 3.11. *Soit A une matrice $m \times n$. Il existe une suite d'opérations élémentaires sur les lignes qui appliquée à A la réduit en une matrice échelonnée réduite A'.*

Démonstration. Il suffit de donner une méthode de réduction : c'est la méthode du pivot de Gauß.

Etape 1 : considérer la première colonne de la matrice. Si cette colonne est nulle, passer à l'étape 2 Si elle est non nulle, choisir une ligne i telle que $a_{i,1}$ soit non nul. Faire $L_i \leftarrow \frac{1}{a_{i,1}} L_i$ puis $L_j \leftarrow L_j - a_{j,1} L_i$ pour $j \neq i$ puis $L_i \leftrightarrow L_j$. A la fin de cette étape, la première colonne de la matrice obtenue est soit nulle, soit de la forme

$$\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Etape 2 : Notons B la matrice obtenue à l'étape 1. On recommance alors l'étape 1 sur la sous matrice obtenue de B en ignorant la première ligne et la première colonne et ainsi de suite. Le nombre de lignes et de colonnes de la matrice considérée à l'étape 1 décroissant strictement, il arrive un moment ou on a plus assez de ligne ou de colonne. La matrice obtenue est alors échelonnée, à savoir, elle vérifie les condition $i)$, $ii)$ et $iii)$ de la définition.

Etape 3 : Soit r le nombre de ligne non nulle. Notons $p(i)$ la position du premier 1 sur la ligne i pour $i = 1, ..., r$. Pour $i = 1, ..., r$, faire $L_j \leftarrow L_j - a_{j,p(i)} L_i$ pour $j = 1, ..., i-1$. □

Exemple. Considérons la matrice

$$\begin{bmatrix} 0 & 1 & -1 & 4 \\ 0 & 2 & 0 & 2 \\ 2 & 4 & -2 & 2 \\ 2 & 1 & -3 & 2 \end{bmatrix}$$

Etape 1 : La première colonne est non nulle. On prend $i = 3$.

$$\begin{bmatrix} 0 & 1 & -1 & 4 \\ 0 & 2 & 0 & 2 \\ 2 & 4 & -2 & 2 \\ 2 & 1 & -3 & 2 \end{bmatrix} \xrightarrow{L_3 \leftarrow \frac{1}{2} L_3} \begin{bmatrix} 0 & 1 & -1 & 4 \\ 0 & 2 & 0 & 2 \\ 1 & 2 & -1 & 1 \\ 2 & 1 & -3 & 2 \end{bmatrix} \xrightarrow{L_4 \leftarrow L_4 - 2L_3} \begin{bmatrix} 0 & 1 & -1 & 4 \\ 0 & 2 & 0 & 2 \\ 1 & 2 & -1 & 1 \\ 0 & -3 & -1 & 0 \end{bmatrix} \xrightarrow{L_1 \leftrightarrow L_3} \begin{bmatrix} 1 & 2 & -1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 1 & -1 & 4 \\ 0 & -3 & -1 & 0 \end{bmatrix}$$

Etape 2 : On considère maintenant la sous matrice

$$\begin{bmatrix} 2 & 0 & 2 \\ 1 & -1 & 4 \\ -3 & -1 & 0 \end{bmatrix} \quad \text{de} \quad \begin{bmatrix} 1 & 2 & -1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 1 & -1 & 4 \\ 0 & -3 & -1 & 0 \end{bmatrix}$$

et on recommence l'étape 1. On prend $i = 1$ dans la sous-matrice et donc $i = 2$ dans la matrice complète.

$$\begin{bmatrix} 1 & 2 & -1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 1 & -1 & 4 \\ 0 & -3 & -1 & 0 \end{bmatrix} \xrightarrow{L_2 \leftarrow \frac{1}{2}L_2} \begin{bmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & -1 & 4 \\ 0 & -3 & -1 & 0 \end{bmatrix} \xrightarrow{L_3 \leftarrow L_3 - L_2} \begin{bmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & -1 & 3 \\ 0 & -3 & -1 & 0 \end{bmatrix} \xrightarrow{L_3 \leftarrow L_3 - L_2} \begin{bmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & -1 & 3 \\ 0 & 0 & -1 & 3 \end{bmatrix}$$

Etape 2 : On considère la sous matrice $\begin{bmatrix} -1 & 3 \\ -1 & 3 \end{bmatrix}$ et on recommence l'étape 1 avec $i = 3$.

$$\begin{bmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & -1 & 3 \\ 0 & 0 & -1 & 3 \end{bmatrix} \xrightarrow{L_3 \leftarrow -L_3} \begin{bmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & -1 & 3 \end{bmatrix} \xrightarrow{L_4 \leftarrow L_4 + L_3} \begin{bmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

La matrice obtenue est échelonnée.
Etape 3 :

$$\begin{bmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{L_1 \leftarrow L_1 - L_2} \begin{bmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{L_1 \leftarrow L_1 + L_3} \begin{bmatrix} 1 & 0 & 0 & -4 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

La matrice obtenue est maintenant échelonnée réduite.

Définition 3.12. Soit S un système linéaire sur k.
$i)$ si S a une solution unique, on dit que S est *régulier*
$ii)$ si S a une infinité de solution, on dit que S est *singulier*
$iii)$ si S n'a pas de solution, on dit que S est non *non-consistant*

Théorème 3.13. *Soit S un système linéaire sur k, alors S est soit régulier, singulier ou non-consistant.*

Démonstration. Soit $M = [A \mid \vec{b}]$ la matrice augmentée de S. Par le théorème 3.11, il existe une suite d'opérations élémentaires sur les lignes qui appliquée à A la réduit en la matrice A'. Si on applique ces opérations sur M, on obtient une matrice augmentée $M' = [A' \mid \vec{b'}]$. D'après la proposition 3.9, le système S' représentée par M' à la même solution que S. Notons r le nombre de lignes non nulles de A' et s le nombre de ligne non-nulles de M'.
Cas $s > r$: aucune solution

$$\left[\begin{array}{ccc|c} 1 & 2 & 0 & -1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{array}\right] \leftrightarrow \begin{cases} x_1 + 2x_2 = -1 \\ x_3 = 2 \\ 0 = 1 \end{cases}$$

Cas $s = r = n$ où n est le nombre d'indeterminé : une solution $x_1 = b'_1, ..., x_n = b'_n$.

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right] \leftrightarrow \begin{cases} x_1 = 3 \\ x_2 = 2 \\ x_3 = 1 \end{cases}$$

Cas $r = s < n$: une infinité de solution car il y'a $n - r$ inderterminées dont le choix est arbitraire.

$$\left[\begin{array}{cccccc|c} 1 & 1 & 2 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 3 & 2 \end{array}\right] \leftrightarrow \begin{cases} x_1 + x_2 + 2x_3 = 1 \\ x_4 + x_6 = -1 \\ x_5 + 3x_6 = 2 \end{cases} \Leftrightarrow \begin{cases} x_1 = 1 - x_2 - 2x_3 = 1 - t_1 - 2t_2 \\ x_4 = -1 - x_6 = 1 - t_3 \\ x_5 = 2 - 3x_6 = 2 - 3t_3 \end{cases}$$

Il y'a trois paramètres dont le choix est arbitraire : t_1, t_2, t_3. $\square$

IV. Groupes et anneaux

1 Groupes

Définition 4.1. Un *Groupe* G est un ensemble non vide muni d'une application $\cdot : G \times G \to G$ appelée *produit* vérifiant

– associativité : pour tout x, y, z de G, on a $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

– existence de neutre : il existe un unique élément $e \in G$ tel que pour tout $x \in G$ on ait $x \cdot e = e \cdot x = x$.

– existence d'inverse : pour tout $x \in G$ il existe un élément $y \in G$ tel qu'on ait $x \cdot y = y \cdot x = e$.

Exemple. $(\mathbb{R}, +)$, $(\mathbb{R}^*)$, $(\mathbb{Z}, +)$.

Proposition 4.2. *Soit $(G, \cdot)$ un groupe alors l'élément neutre est unique et pour tout $x \in G$ il existe un unique $y \in G$ vérifiant $x \cdot y = y \cdot x = e$.*

Démonstration. Soit e et f deux éléments neutres Comme e est un neutre, on a $e \cdot f = f$. De même, comme f est neutre, on a $e \cdot f = e$. On en déduit $e = f$.

Soit x un élément de G. Montrons que l'inverse de x est unique. Soit y un élément de G vérifiant $x \cdot y = y \cdot x = e$ et z un élément de G vérifiant $x \cdot z = z \cdot x = e$ Comme e est neutre, on a $z \cdot e = z \cdot (x \cdot y) = (z \cdot x) \cdot y = e \cdot y = y$. □

Définition 4.3. L'élément y introduit à la définition 4.1 et dont l'unicité est prouvé à la proposition 4.2 est appelée *inverse de* x et est notée x^{-1}.

Définition 4.4. On dit qu'un groupe $(G, \cdot)$ est *commutatif* ou *abélien* si son produit est commutatif : pour tout x, y de G, on a $x \cdot y = y \cdot x$.

Pour certains groupes commutatifs, on note le produit par $+$, l'élément neutre par 0 et l'inverse de x par $-x$.

Exemple. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C}^*, \cdot)$.

Lemme 4.5. *Soit $(G, \cdot)$ un groupe et x, y, z des éléments de G. On a*

– $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$

– $x \cdot z = y \cdot z$ *implique* $x = y$

– $z \cdot x = z \cdot y$ *implique* $x = y$

Démonstration. Pour la première relation, on montre

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = x \cdot (y \cdot (y^{-1} \cdot x^{-1}) = x \cdot ((y \cdot y^{-1}) \cdot x^{-1}) = x \cdot (e \cdot x^{-1}) = x \cdot x^{-1} = e$$
$$(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = ((y^{-1} \cdot x^{-1}) \cdot x) \cdot y = (y^{-1} \cdot (x^{-1} \cdot x)) \cdot y = (y^{-1} \cdot e) \cdot y = y^{-1} \cdot y = e$$

Pour la deuxième, on montre

$$x = x \cdot e = x \cdot (z \cdot z^{-1}) = (x \cdot z) \cdot z^{-1} = (y \cdot z) \cdot z^{-1} = y \cdot (z \cdot z^{-1}) = y \cdot e = y$$

Pour la troisième, on montre

$$x = e \cdot x = (z^{-1} \cdot z) \cdot x = z^{-1} \cdot (z \cdot x) = z^{-1} \cdot (z \cdot y) = (z^{-1} \cdot z) \cdot y = e \cdot y = y$$

□

Définition 4.6. Soit $(G, \cdot)$ un groupe. On dit qu'une partie $H \subseteq G$ est un *sous-groupe* de G si H muni de de la restriction de $\cdot$ à $H \times H$ est lui-même un groupe.

Proposition 4.7. *Soit $(G, \cdot)$ un groupe. Une partie H non vide de G est un sous-groupe de G, si on a*

$i)$ pour tout x, y de H, on a $x \cdot_G y \in H$

$ii)$ pour tout x de H, on $x^{-1} \in H$.

Démonstration. Notons $\cdot_H$ la restriction de $\cdot_G$ à $H \times H$. Par $i)$ on a bien $\cdot_H : H \times H \to H$. L'application $\cdot_H$ est associative car $\cdot_G$ l'est. Soit x un élément de H, comme x est aussi un élément de G , il admet un inverse x^{-1} dans G qui se trouve être un élément de H par $ii)$.

Soit e l'élément neutre de G et x un élément de H. Alors on a $e \cdot_H x = e \cdot_G x = x$ et $x \cdot_H e = x \cdot_G e = x$, d'où $e \cdot_H x = x \cdot_H e = x$. Mais e est-il un élément de H ? Oui car par $ii)$, on a $x^{-1} \in H$ et donc par $i)$, on a $e = x \cdot x^{-1} \in H$.

□

Exemple.

– L'ensemble des entiers divisibles par 2 est un sous groupe de $(\mathbb{Z}, +)$

– L'ensemble des entiers non divisibles par 2 n'est pas un sous groupe de $(\mathbb{Z}, +)$

– L'ensemble des racine n-ièmes de l'unité, muni du produit de $\mathbb{C}$ est un sous-groupe de $(\mathbb{C}^*, \cdot)$.

Définition 4.8. Soient $(G, \cdot_G)$ et $(H, \cdot_H)$ deux groupes. Un *morphisme de groupes de G dans H* est une application $\phi : G \to H$ vérifiant :

$$\forall a, b \in G \quad \phi(a \cdot_G b) = \phi(a) \cdot_H \phi(b)$$

Si ϕ est de plus surjective ; on dit que ϕ est un *isomorphisme* de groupes.

Exemple.

$$\begin{aligned} \phi = (\mathbb{R}, \cdot) &\to (\mathbb{R}^*, \cdot) \\ a &\mapsto e^a \end{aligned}$$

est un morphisme ($e^{a+b} = e^a \cdot e^a$) mais ce n'est pas un isomorphisme car $\phi(\mathbb{R}) \neq \mathbb{R}$.

Proposition 4.9. *Soient $(G, \cdot_G)$ et $(H, \cdot_H)$ deux groupes et ϕun morphisme de G dans H. Alors on a $\phi(e_G) = e_H$ et pour tout x de G on a $\phi(x^{-1}) = \phi(x)^{-1}$.*

Démonstration. Soit x un élément de G, on a alors

$$e_H \cdot \phi(x) = \phi(x) = \phi(e_G \cdot x) = \phi(e_G)\phi(x),$$

ce qui implique $\phi(e_G) = e_H$ par le lemme 4.5 Pour l'autre relation, on établie

$$\phi(x) \cdot \phi(x)^{-1} = e_H = \phi(e_G) = \phi(x \cdot x^{-1}) = \phi(x) \cdot \phi(x^{-1})$$

et donc $\phi(x)^{-1} = \phi(x^{-1})$ d'après le lemme 4.5.

□

2 Anneau

Définition 4.10. Un anneau A est un ensemble non vide muni de 2 opérations $+_A : A \times A \to A$, $\cdot_A : A \times A \to A$ vérifiant :

$i)$ $(A, +_A)$ est un groupe commutatif dont l'élément neutre est noté 0_A.

$ii)$ associativité du produit : pour tout x, y, z de A, on a $x \cdot_A (y \cdot_A z) = (x \cdot_A y) \cdot_A z$

$iii)$ existence de neutre pour $\cdot_A$ (noté 1_A) : pour tout $x \in A$, on a $x \cdot_A 1_A = 1_A \cdot_A x = x$.

$iv)$ distributivité de $\cdot$ sur $+$: pour tout $x, y, z \in A$, on a $x \cdot_A (y +_A z) = x \cdot_A y +_A x \cdot_A z$ et $(y +_A z) \cdot_A x = y \cdot_A x +_A z \cdot_A x$.

Définition 4.11. On dit qu'un anneau $(A, +_A, \cdot_A)$ est commutatif si le produit $\cdot_A$ est commutatif : $\forall x, y \in A(x \cdot_A y = y \cdot_A x)$.

Exemple. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{Z}[X], +, \times)$, $(\mathbb{Q}[X], +, \times)$, $(\mathbb{R}[X], +, \times)$, $(\mathbb{C}[X], +, \times)$ sont des anneaux commutatifs.

Définition 4.12. Soient $(A, +_A, \cdot_A)$ et $(B, +_B, \cdot_B)$ deux anneaux. Une application $\phi : A \to B$ est un *morphisme d'anneaux* si pour tout $x, y \in A$, on a

$i)$ $\phi(x +_A y) = \phi(x) +_B \phi(y)$

$ii)$ $\phi(x \cdot_A y) = \phi(x) \cdot_B \phi(y)$

On ne demande pas l'existence d'inverse pour le produit. Par exemple le polynôme x n'admet pas d'inverse pour $\times$ dans $(\mathbb{Q}[X], +, \times)$.

Définition 4.13. Soit $(A, +_A, \cdot_A)$ un anneau. On dit qu'un élément x de A^* est inversible s'il existe $y \in A$ tel que $x \cdot_A y = y \cdot_A x = 1_A$. L'ensemble des éléments inversibles de A est noté A^*.

Lemme 4.14. *Soit $(A, +_A, \cdot_A)$ un anneau. Alors $(A^*, \cdot_A)$ est un groupe, appellé* groupe multiplicatif *de A*

Démonstration. Montrons que $\cdot_A$ est une loi de A^*. Soient a, b des éléments de A^*. Alors on a $(a \cdot_A b) \cdot_A (b^{-1} \cdot a^{-1}) = a \cdot_A 1_A \cdot_A a^{-1} = 1_A$ et $(b^{-1} \cdot_A a^{-1}) \cdot_A (a \cdot b) = b^{-1} \cdot_A 1_A \cdot_A b = 1_A$. L'associativité et l'existence de neutre découlent des propriétés d'anneaux de A. L'existence d'inverse est l'hypothèse de définition. $\square$

Exemple.

- $(\mathbb{Z}, +, \times)^* = \{-1, 1\}$,
- $(\mathbb{Q}, +, \times)^* = \mathbb{Q} \setminus \{0\}$,
- $(\mathbb{R}[X], +, \times)^* = \mathbb{R} \setminus \{0\}$.

La situation idéale est celle ou chaque élément non nul est inversible.

Définition 4.15. Un corps k est un anneau commutatif tele que $k^* = k \setminus \{0\}$

Exemple. $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ sont des corps.

3 Cas des matrices

Définition 4.16. L'ensemble des matrices à m lignes et n colonnes à coefficient dans un corps $\mathbb{K}$ et notées $M_{m,n}(\mathbb{K})$

Définition 4.17. Soient $A = (a_{i,j})$ et $B = (b_{i,j})$ deux matrices de $M_{m,n}(\mathbb{K})$. On définit l'addition matricielle $+ : M_{m,n}(\mathbb{K}) \times M_{m,n}(\mathbb{K}) \to M_{m,n}(\mathbb{K})$ en posant

$$A + B = (a_{i,j} +_{\mathbb{K}} b_{i,j})$$

Exemple.

$$\begin{bmatrix} 0 & -1 & 3 & 4 \\ 1 & 2 & -3 & 4 \end{bmatrix} + \begin{bmatrix} 1 & 2 & 0 & 0 \\ -1 & 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 3 & 4 \\ 0 & 5 & -1 & 5 \end{bmatrix}$$

Proposition 4.18. *L'ensemble $M_{m,n}(\mathbb{K})$ munis de l'addition matricielle forme un groupe commutatif. De plus l'élément neutre est la matrice de $M_{m,n}(\mathbb{K})$ dont tous les coefficients sont $0_{\mathbb{K}}$.*

Démonstration. L'addition matricielle est bien une loi interne de $M_{m,n}(\mathbb{K})$. Soient A, B et C des matrices de $M_{m,n}(\mathbb{K})$. Alors on a

$$A + (B + C) = A + ({}_{\mathbb{K}}b_{i,j} +_{\mathbb{K}} c_{i,j}) = (a_{i,j} +_{\mathbb{K}} (b_{i,j} +_{\mathbb{K}} c_{i,j}))$$

ainsi que

$$(A + B) + C = (a_{i,j} +_{\mathbb{K}} b_{i,j}) +_{\mathbb{K}} C = ((a_{i,j} +_{\mathbb{K}} b_{i,j}) +_{\mathbb{K}} c_{i,j})$$

L'addition étant associative dans le corps $\mathbb{K}$ (qui est un anneau particulier), on a

$$a_{i,j} +_{\mathbb{K}} (b_{i,j} +_{\mathbb{K}} c_{i,j}) = (a_{i,j} +_{\mathbb{K}} b_{i,j}) +_{\mathbb{K}} c_{i,j} \quad \text{pour tout } 1 \leqslant i \leqslant m \text{ et } 1 \leqslant j \leqslant n,$$

ce qui implique $(A + B) + C = A + (B + C)$. Soit $0_{m,n}$ la matrice dont tous les coefficients sont nuls. Alors pour tout $A = (a_{i,j}) \in M_{m,n}(\mathbb{K})$ on a

$$A + 0_{m,n} = (a_{i,j} +_{\mathbb{K}} 0) = (a_{i,j}) = A \quad \text{et} \quad 0_{m,n} + A = (0 +_{\mathbb{K}} a_{i,j}) = (a_{i,j}) = A$$

Soit $A = (a_{i,j})$ une matrice de $M_{m,n}(\mathbb{K})$, on pose $-A = (-a_{i,j})$. On a a alors

$$A + (-A) = (a_{i,j} +_{\mathbb{K}} (-a_{i,j}) = (0) = 0_{m,n} \quad \text{et}(-A) + A = (-a_{i,j} +_{\mathbb{K}} a_{i,j}) = (0) = 0_{m,n}.$$

Soient A et B deux matrice de $M_{m,n}(K)$. L'addition $+_{\mathbb{K}}$ étant commutative, on vérifie

$$A + B = (a_{i,j} +_{\mathbb{K}} b_{i,j}) = (b_{i,j} +_{\mathbb{K}} a_{i,j}) = B + A.$$

□

Définition 4.19. Soit A une matrice de $M_{m,n}$ et B une matrice de $M_{n,p}$. On définit le produit matriciel $A \times B$ par

$$A \times B = (C_{i,j})_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant p} \quad \text{avec} \quad c_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,i}$$

On a déjà vu ce produit dans le chapitre “système linéaire” dans le cas ou B est un vecteur, c'est-à-dire, une matrice $M_{n,1}$.

Exemple.

$$\begin{bmatrix} 0 & -1 & 3 & 4 \\ 1 & 2 & -3 & 4 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & -1 & -1 \\ -1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} -5 & -5 & -4 \\ -1 & 8 & 5 \end{bmatrix}$$

Le produit matricielle n'est pas une loi interne de $M_{m,n}(\mathbb{K})$ en général. En Effet il faut que le nombre de ligne de la matrice de gauche coincide avec le nombre cde colonnes de la mattice de droite.

Définition 4.20. Une matrice est dite carré si elle a autant de ligne que de colonne. L'ensemble des matrices carrées de taille n est noté $M_n(\mathbb{K})$.

On a donc $M_n(\mathbb{K}) = M_{n,n}(\mathbb{K})$.

Définition 4.21. La matrice identité I_n est la matrice de $M_n(\mathbb{K})$ dons tous les coefficients sont $0_{\mathbb{K}}$ sauf ceux sur la diagonale qui vallent $1_{\mathbb{K}}$

Exemple.

$$I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Proposition 4.22. $(M_n(\mathbb{K}), +, \times)$ *est un anneau qui a* $0_{n,n} = 0_n$ *comme* 0 *et* I_n *comme unité.*

Démonstration. On a déjà montré que $(M_n(\mathbb{K}), +)$ est un groupe d'élément neutre 0_n.

L'opération $\times$ est bien une loi interne de $M_n(\mathbb{K})$

Associativité : Soient A, B et C trois matrices de $M_n(\mathbb{K})$. On a alors

$$A \times (B \times C) = A \times \left(\sum_{k=1}^{n} b_{i,k} c_{k,j} \right) = \left(\sum_{\ell=1}^{n} a_{i,\ell} \sum_{k=1}^{n} b_{\ell,k} c_{k,j} \right) = \left(\sum_{\ell=1}^{n} \sum_{k=1}^{n} b_{\ell,k} a_{i,\ell} c_{k,j} \right)$$

$$(A \times B) \times C = \left(\sum_{k=1}^{n} a_{i,k} b_{k,j} \right) \times C = \left(\sum_{\ell=1}^{n} \left(\sum_{k=1}^{n} a_{i,k} b_{k,\ell} \right) c_{\ell,j} \right) = \left(\sum_{\ell=1}^{n} \sum_{k=1}^{n} a_{i,k} b_{k,\ell} c_{\ell,j} \right)$$

La loi $\times$ est donc associative.

Neutre : Le symbole de Kronecker δ_i^j est définie par $\delta_i^j = 1$ si $i = j$ et 0 sinon. Soit A une matrice de $M_n(\mathbb{K})$. On a

$$A \times I_n = \left(\sum_{k=1}^{n} A_{i,k} \delta_k^j \right) = (a_{i,j}) = A$$

ainsi que

$$A \times I_n = \left(\sum_{k=1}^{n} \delta_i^k A_{k,j} \right) = (a_{i,j}) = A$$

Distributivité : Soient A, B et C trois matrices de $M_n(\mathbb{K})$. On a

$$A \times (B + C) = A \times (b_{i,j} + c_{i,j}) = \left(\sum_{k=1}^{n} a_{i,k} (b_{k,j} + c_{k,j}) \right) = \left(\sum_{k=1}^{n} a_{i,k} b_{k,j} + a_{i,k} c_{k,j} \right)$$

$$= \left(\sum_{k=1}^{n} a_{i,k} b_{k,j} \right) + \left(\sum_{k=1}^{n} a_{i,k} c_{k,j} \right) = AB + AC.$$

De même pour $(B + C) \times A$. $\square$

Attention, le produit matriciel n'est pas commutatif.
Quaestion : Quelles sont les matrices inversibles ?

Exemple. On a

$$\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix} \neq \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$$

Définition 4.23. On définit les matrices *élémentaires* $E_{i,j}$ avec $1 \leqslant i \neq j \leqslant n$, $E_i(\alpha)$ avec $1 \leqslant i \leqslant n$ et $\alpha \in \mathbb{K}$ et $E_{i,j}(\alpha)$ avec $1 \leqslant i \neq j \leqslant n$ et $\alpha \in \mathbb{K}$ par

Proposition 4.24. *Soit A une matrice de $M_n(\mathbb{K})$. Faire une opération élementaire de ligne sur A revient à multiplier A à gauche par une des matrices élémentaires.*

Exemple. –$L_1 \leftrightarrow L_2$

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 3 & 0 \\ 1 & 2 & 1 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 3 & 0 \\ 0 & -1 & -1 \end{bmatrix}$$

– $L_3 \leftarrow 5L_3$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{bmatrix} \begin{bmatrix} 1 & 3 & 0 \\ 1 & 2 & 1 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 3 & 0 \\ 1 & 2 & 1 \\ 0 & -5 & -5 \end{bmatrix}$$

– $L_1 \leftarrow L_1 + 2L_2$

$$\begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 3 & 0 \\ 1 & 2 & 1 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 3 & 7 & 2 \\ 1 & 2 & 1 \\ 0 & -1 & -1 \end{bmatrix}$$

Lemme 4.25. *Les matrices élémentaires de $M_n(\mathbb{K})$ sont inversibles.*

Démonstration. On a $E_{i,j}^{-1} = E_{i,j}$, $E_i(\alpha)^{-1} = E_i\left(\frac{1}{\alpha}\right)$ et $E_{i,j}(\alpha) = E_{i,j}(-\alpha)$. □

Lemme 4.26. *Soit A une matrice de $M_n(\mathbb{K})$ et B une matrice obtenue de A par une opération élémentaire sur les lignes. Alors A est inversible si et seulement si B est inversible.*

Démonstration. D'après, la proposition .**??**, il existe une matrice élémentaire E tel qu'on ait $B = EA$. Comme E est inversible, on a $A = E^{-1}B$. L'ensemble des éléments inversibles d'un anneau formant un groupe et E (ainsi que E^{-1} étant inversible), on en déduit que $B = EA$ est inversible si A l'est et $A = E^{-1}B$ est inversbile si B l'est. □

Lemme 4.27. *La seule matrice échelonnée réduite inversible de $M_n(\mathbb{K})$ est I_n.*

Démonstration. Soit A une matrice échelonnée réduite de $M_n(\mathbb{K})$. Si la ligne i de A est nulle alors la ligne i de $C = AB$ est nulle pour tout B de $M_n(\mathbb{K})$ car on aurait

$$C_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j} = \sum_{k=1}^{n} 0 = 0 \quad \forall j$$

Il ne peut donc pas exister de matrice B vérifiant $AB = I_n$. Supposons maintenant que toutes les lignes de A sont non nulles. Notons $p(k)$ la position du premier 1 de la ligne k. Comme A est une matrice carré de taille n échelonnée, on a $1 \leqslant p(1) \leqslant p(2) \leqslant ... \leqslant p(n) \leqslant n$, Ce qui implique $p(k) = k$ pour tout $k = 1, ..., n$ puis $A = I_n$.

□

Théorème 4.28. *Une matrice A de $M_n(\mathbb{K})$ est inversible si et seulement si la matrice échelonnée réduite obtenue de A est I_n.*

Démonstration. Soit A une matrice de $M_n(\mathbb{K})$. Notons B la matrice échelonnée réduite obtenue de A. Par le lemme .**??**, la matrice A est inversible si et seulement si B est inversible. Or par le lemme .**??**, la seule matrice échelonnée réduite inversible est I_n. □

Proposition 4.29. *Soit A une matrice de $M_n(\mathbb{K})$. Si la méthode du pivot de Gaußappliqué à la matice augmentée $(A|I_n)$ retourne $(I_n|B)$ alors la matrice A est inversible et d'iverse B.*

Démonstration. Le fait que A soit inversible est exactement le théorème précédent. Appliquer la méthode du pivot de Gaußrevient à mulitplier A par des matrices élémentaires. On a alors $E_rE_{r-1}....E_2E_1A = I_n$ et donc $E_rE_{r-1}....E_2E_1(A|I_n) = (I_n|E_rE_{r-1}....E_2E_1)$. En posant $C = E_rE_{r-1}....E_2E_1$, on a $CA = I_n$ et $C(A|I_n) = (I_n|C)$. Ce qui montre que $B = C$ est l'inverse de A si on établi aussi $AC = I_n$. Nous le faisons pas pour le moment, mais un argument théorique utltérieur permettera de conclure. □

Exemple. Calculer l'inverse de

$$\begin{bmatrix} 5 & 2 & 1 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix} \quad \text{qui est} \quad \begin{bmatrix} 1 & -2 & -1 \\ -1 & 3 & 1 \\ -2 & 4 & 3 \end{bmatrix}$$

V. Espace vectoriel

1 Espaces et sous-espaces vectoriels

Définition 5.1. Soit $\mathbb{K}$ un corps $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots)$. Un $\mathbb{K}$-espace vectoriel E c'est un ensemble muni de deux opérations :

- Une opération interne de E, notée $+_E$, et vérifiant
  $a)$ Associativité $\forall \vec{u}, \vec{v}, \vec{w} \in E,\ (\vec{u} + \vec{v}) +_E \vec{w} = \vec{u} +_E (\vec{v} +_E \vec{w})$
  $b)$ Existence d'un neutre : $\exists \vec{0} \in E,\ (\forall \vec{u} \in E,\ \vec{0} +_E \vec{u} = \vec{u} +_E \vec{0} = \vec{u})$
  $c)$ Existence d'opposée : $\forall \vec{u} \in E, \exists \vec{v} \in E, \vec{u} +_E \vec{v} = \vec{v} +_E \vec{u} = \vec{0}$
  $d)$ Commutativité : $\forall \vec{u}, \vec{v} \in E, \vec{u} +_E \vec{v} = \vec{v} +_E \vec{u}$
- Une opération externe de $\mathbb{K}$ sur E, notée $\cdot_E$, et vérifiant
  $e)$ $\forall \vec{u} \in E, 1 \cdot_E \vec{u} = \vec{u}$
  $f)$ $\forall \vec{u} \in E, \forall \lambda, \mu \in \mathbb{K},\ (\lambda +_E \mu) \cdot_E \vec{u} = \lambda \cdot_E \vec{u} +_E \mu \cdot_E \vec{u}$
  $g)$ $\forall \vec{u} \in E, \forall \lambda, \mu \in \mathbb{K},\ (\lambda \cdot_{\mathbb{K}} \mu) \cdot_E \vec{u} = \lambda \cdot_E (\mu \cdot_E \vec{u})$
  $h)$ $\forall \vec{u}, \vec{v} \in E, \forall \lambda \in \mathbb{K},\ \lambda \cdot_E (\vec{u} +_E \vec{v}) = \lambda \cdot_E \vec{u} +_E \lambda \cdot_E \vec{v}$

Remarque 5.2. – On utilise la terminologie de $\mathbb{K}$-espace vectoriel au lieu de espace vectoriel sur un corps $\mathbb{K}$.
– Les éléments de E sont les vecteurs de E.
– $\forall \vec{u} \in E, \vec{0} \cdot_E \vec{u} = \vec{0}$.
– $\forall \lambda \in \mathbb{K}, \lambda \cdot_E \vec{0} = \vec{0}$.
– $(-1) \cdot_E \vec{u} = -\vec{u}$, l'inverse de $\vec{u}$ pour $+_E$.

Exemple. $E = \mathbb{R}^n$, l'ensemble des colonnes de taille n muni des opérations

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} +_E \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{bmatrix}$$

$$\lambda \cdot_E \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \lambda \cdot x_1 \\ \vdots \\ \lambda \cdot y_n \end{bmatrix}$$

est un espace vectoriel sur $\mathbb{R}$. En particulier le plan $\mathbb{R}^2$ est un espace vectoriel (dessin deux vecteur et règle parralélogramme)

$\mathbb{C}[X]$ est un espace vectoriel pour les opérations
– $+$: somme de deux polynômes
– $\forall \lambda \in \mathbb{C}$, $\lambda \cdot (a_n X^n + \ldots + a_1 x + a_0) = \lambda a_n x^n + \ldots + \lambda a_1 x + \lambda a_0$.

Définition 5.3. Soit E un $\mathbb{K}$-espace vectoriel. Un *sous-espace* vectoriel F de E est un sous ensemble de E qui avec les opérations de E est lui même un espace vectoriel.

Proposition 5.4. *F est un sous-espace vectoriel de E si*
$a)$ $\forall \vec{w}_1, \vec{w}_2 \in W,\ \vec{w}_1 +_E \vec{w}_2 \in F$
$b)$ $\forall \vec{w} \in W, \forall \lambda \in \mathbb{K},\ \lambda \cdot_E \vec{w} \in F$

Démonstration. On définit

$$\begin{aligned} +_F : F \times F &\to F \\ (\vec{u}\,, \vec{v}) &\mapsto \vec{u} +_E \vec{v} \end{aligned} \qquad\qquad \begin{aligned} \cdot_F : \mathbb{K} \times F &\to F \\ (\lambda\,, \vec{u}) &\mapsto \lambda \cdot_E \vec{u} \end{aligned}$$

Ces lois sont biens définies d'après le $a)$ et $b)$. Comme $+_E$ et $\cdot_F$ vérifient les conditions $a), \dots, h)$ de la défintion 5.1, il en est de même pour $+_F$ et $\cdot_F$. □

Exemple. Les sous espaces vectoriels de $\mathbb{R}^2$ sont :
- $\{0\}$;
- les droites passant par $\{0\}$ [dessin] ;
- $\mathbb{R}^2$ lui même.

Dans $\mathbb{R}^3$, un plan est un sous-espace vectoriel si et seulement si ce plan passe par l'origine. N'importe quel sous-espace vectoriel contient $\vec{0}$.

2 Familles génératrices et libres

Définition 5.5. Soit E un $\mathbb{K}$-espace vectoriel. Une *combinaison linéaire* en les vecteurs $\vec{u}_1, \dots, \vec{u}_k$ de E est un vecteur $\vec{u} = \lambda_1 \vec{u}_1 + \ldots + \lambda_k \vec{u}_k$, où les λ_i sont des éléments de $\mathbb{K}$.

Proposition 5.6. *Un $\mathbb{K}$-espace vectoriel E contient toutes les combinaisons linéaires en ses éléments.*

Démonstration. La loi externe $\cdot_E$ de E est une application $\mathbb{K} \times E \to E$, en particulier elle est à image dans E. Ainsi $\lambda_i \cdot_E \vec{u}_i$ appartient à E pour $i = 1, \dots, k$. Comme la loi $+_E$ est une loi interne de E la somme de deux vecteurs de E est dans E , il en est donc de même pour le vecteur $\lambda_1 \cdot_E \vec{u}_1 +_E \ldots +_E \lambda_k \cdot_E \vec{u}_k$. □

Définition 5.7. On dit que $\mathcal{F} = \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\}$ est une famille génératrice d'un $\mathbb{K}$-espace vectoriel E si tout $\vec{v}$ de E est combinaison linéaire de vecteurs de $\mathcal{F}$. Dans ce cas, on dit que E est engendré par $\mathcal{F}$ et on note $E = \mathrm{Vect}_{\mathbb{K}}(\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n)$.

Exemple. E : le plan (XY) de $\mathbb{R}^3$, $\vec{u}_1 = \begin{bmatrix} 1 & -1 & 0 \end{bmatrix}$, $\vec{u}_2 = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}$. La famille $\{\vec{u}_1, \vec{u}_2\}$ est une famille libre de E.

Soit $\vec{v} = \begin{bmatrix} 3 & 3 & 0 \end{bmatrix}$. Comme $\{\vec{u}_1, \vec{u}_2\}$ est une famille génératrice de E, il existe $\lambda_1, \lambda_2 \in \mathbb{R}$ tel que

$$\vec{v} = \lambda_1 \vec{u}_1 + \lambda_2 \vec{u}_2 = \lambda_1 \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} + \lambda_2 \begin{bmatrix} 1 & 2 & 0 \end{bmatrix} = \begin{bmatrix} \lambda_1 + \lambda_2 \\ -\lambda_1 + 2\lambda_2 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 & 3 & 0 \end{bmatrix}$$

En résolvant le système, on trouve $\lambda_1 = 1$ et $\lambda_2 = 2$.

La famille $\{\vec{u}_1, \vec{v}_1, \vec{v}\}$ est aussi une famille génératrice du plan (XY).

Problème : $\vec{0} = 0 \cdot \vec{u}_1 + 0 \cdot \vec{u}_2 + 0 \cdot \vec{u}_3$ et $\vec{0} = -\vec{u}_1 - 2\vec{u}_2 + \vec{v}$.

Il n'y pas unicité de "l'écriture".

La définition suivante évite ce genre de situation.

Définition 5.8. On dit que $\{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n\}$ est une *famille libre* d'un $\mathbb{K}$-espace vectoriel E si :

$$\lambda_1 \cdot_E \vec{u}_1 +_E \lambda_2 \cdot_E \vec{u}_2 +_E \ldots +_E \lambda_k \cdot_E \vec{u}_k = \vec{0} \Rightarrow \lambda_1 = \lambda_2 = \ldots = \lambda_k = 0.$$

Autrement dit, il n'y a qu'une seule combinaison linéaire en les vecteurs de $\mathcal{F}$ qui donne le vecteur nul.

Proposition 5.9. *Soit $\mathcal{F} = \{\vec{u}_1, ..., \vec{u}_\ell\}$ une famille libre d'un $\mathbb{K}$-espace vectoriel E. Chaque $\vec{v} \in Vect_{\mathbb{K}}(\mathcal{F})$ s'écrit de manière unique comme combinaison linéaire en les $\vec{u}_i$.*

Démonstration. Supposons $\vec{v} = \lambda_1 \cdot_E \vec{u}_1 +_E ... +_E \lambda_\ell \cdot_E \vec{u}_\ell$ et $\vec{v} = \mu_1 \cdot_E \vec{u}_1 +_E ... +_E \mu_\ell \cdot_E \vec{u}_\ell$. Il vient

$$\vec{0} = \vec{u} - \vec{u} = \lambda_1 \cdot_E \vec{u}_1 +_E ... +_E \lambda_\ell \cdot_E \vec{u}_\ell - (\mu_1 \cdot_E \vec{u}_1 +_E ... +_E \mu_\ell \cdot_E \vec{u}_\ell) = (\lambda_1 - \mu_1) \cdot_E \vec{u}_1 +_E ... +_E (\lambda_\ell - \mu_\ell) \cdot_E \vec{u}_\ell.$$

Ce qui par définition d'une famille libre implique $\lambda_k - \mu_k = 0$ pour tout $k = 1, ..., \ell$ et donc $\lambda_k = \mu_k$ pour tout k.

□

Proposition 5.10. *Soit $\mathcal{F} = \{\vec{u}_1, ..., \vec{u}_\ell\}$ une famille libre d'un $\mathbb{K}$-espace vectoriel E. Alors aucun des $\vec{u}_i$ n'est combinaison linéaire des autres $\vec{u}_k$ avec $k \neq i$.*

Démonstration. Par l'absurde, supposons $\vec{u}_i = \lambda_1 \cdot_E \vec{u}_1 +_E ... +_E \lambda_{i-1} \cdot_E \vec{u}_{i-1} + \lambda_{i+1} \cdot_E \vec{u}_{i+1} +_E ... +_E \lambda_\ell \cdot_E \vec{u}_\ell$. Alors on a

$$\vec{0} = \lambda_1 \cdot_E \vec{u}_1 +_E ... +_E \lambda_{i-1} \cdot_E \vec{u}_{i-1} - \vec{u}_i +_E \lambda_{i+1} \cdot_E \vec{u}_{i+1} +_E ... +_E \lambda_\ell \cdot_E \vec{u}_\ell,$$

ce qui implique $\lambda_1 = ... = \lambda_{i-1} = -1 = \lambda_{i+1} = ... = \lambda_\ell = 0$ qui est impossible. □

Pour le moment on a juste vu des conséquences de la définition d'une famille libre. En fait, on montre

Proposition 5.11. *Soit E un $\mathbb{K}$-espace vectoriel et $\mathcal{F} = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n\}$ une famille de vecteur de non nul E. Alors il y'a équivalence entre*

$a)$ $\mathcal{F}$ est libre

$b)$ $\lambda_1 \cdot_E \vec{u}_1 +_E \ldots +_E \lambda_k \cdot_E \vec{u}_k = \mu_1 \cdot_E \vec{u}_1 +_E \ldots +_E \mu_k \cdot_E \vec{u}_k$ implique $\lambda_i = \mu_i$ pour $i = 1, \ldots, k$.

$c)$ Aucun $\vec{u}_i$ n'est combinaison linéaire en les autres $\vec{u}_j$.

Démonstration. Les implications $a) \Rightarrow b)$ et $a) \Rightarrow c)$ sont des conséquences directes des deux propositions précédentes. Montrons $b) \Rightarrow a)$. Soient $\lambda_1, ..., \lambda_\ell$ telles que

$$\vec{0} = \lambda_1 \cdot_E \vec{u}_1 +_E ... +_E \lambda_\ell \cdot_E \vec{u}_\ell.$$

On peut aussi écrire $\vec{0} = 0 \cdot_E \vec{u}_1 +_E ... +_E 0 \cdot_E \vec{u}_\ell$. Ce qui, par le $b)$ donne $\lambda_1 = 0, ..., \lambda_\ell = 0$. Montrons $c) \Rightarrow a)$. Supposons qu'on ait $\lambda_1 \cdot_E \vec{u}_1 +_E \lambda_2 \cdot_E \vec{u}_2 +_E \ldots +_E \lambda_k \cdot_E \vec{u}_k = \vec{0}$ et que les λ_i ne soient pas tous nul. Il existe dons i de $\{1, \ldots, k\}$ tels que λ_1 soit non nul. On a donc

$$-\lambda_i \cdot_E \vec{u}_i = \lambda_1 \cdot_E \vec{u}_1 +_E \ldots +_E \lambda_{i-1} \cdot_E \vec{u}_{i-1} +_E \lambda_{i+1} \cdot_E \vec{u}_{i+1} +_E \ldots +_E \lambda_k \cdot_E \vec{u}_k$$

et donc, comme $\lambda_i \neq 0$,

$$\vec{u}_i = -\frac{\lambda_1}{\lambda_i} \cdot_E \vec{u}_1 +_E \ldots +_E -\frac{\lambda_{i-1}}{\lambda_i} \cdot_E \vec{u}_{i-1} +_E -\frac{\lambda_{i+1}}{\lambda_i} \cdot_E \vec{u}_{i+1} +_E \ldots +_E -\frac{\lambda_k}{\lambda_i} \cdot_E \vec{u}_k,$$

ce qui n'es pas possible par $c)$. On a donc nécessairement $\lambda_1 = \ldots = \lambda_k = 0$. □

3 Bases

Définition 5.12. Une base $\mathcal{B}$ d'un $\mathbb{K}$-espace vectoriel E est une famille de E qui est à la fois libre et génératrice.

Exemple. 1)

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad e_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

est une base de $\mathbb{R}^3$. De manière générale la famille $\mathcal{B} = \{e_1, .., e_n\}$ est une base de $\mathbb{R}^n$, c'est la base canonique.

2) Posons $E = \mathbb{C}[X]_{\leqslant n}$ les polynômes à coefficients complexes de degré $\leqslant n$. Les monômes $1, X, ..., X^n$ forment une base de E.

Lemme 5.13. *Si $\mathcal{F} = \{\vec{u}_1, \ldots, \vec{u}_n\}$ est une famille génératrice d'un $\mathbb{K}$-espace vectoriel E composée de vecteur non nul et qui n'est pas libre, alors :*

$a)$ il existe $1 \leqslant i \leqslant n$ tel que $\vec{u}_i$ soit combinaison linéaire en les $\{\vec{u}_1, \ldots, \vec{u}_{i-1}\}$.

$b)$ la famille $\mathcal{F} \setminus \{\vec{u}_i\}$ est encore génératrice.

Démonstration. Montrons $a)$. Comme $\mathcal{F}$ est non libre, il existent des λ_i de $\mathbb{K}$ non tous nuls tels que

$$\lambda_1 \cdot_E \vec{u}_1 +_E \lambda_2 \cdot_E \vec{u}_2 +_E \ldots +_E \lambda_k \cdot_E \vec{u}_k = \vec{0}$$

Soit i le plus grand indice tel que λ_i soit différent de 0. Par construction de i, on a

$$-\lambda_i \cdot_E \vec{u}_i = \lambda_1 \cdot_E \vec{u}_1 +_E \ldots +_E \lambda_{i-1} \cdot_E \vec{u}_{i-1}$$

puis, comme $\lambda_i \neq 0$

$$\vec{u}_i = -\frac{\lambda_1}{\lambda_i} \cdot_E \vec{u}_1 +_E \ldots +_E -\frac{\lambda_{i-1}}{\lambda_i} \cdot_E \vec{u}_{i-1}.$$

Pour $j = 1, \ldots, i-1$, posons $\mu_j = -\frac{\lambda_j}{\lambda_i}$. Pour le $b)$, montrons que toute combinaisons linéaires en les vecteurs de $\mathcal{F}$ est aussi une combinaison linéaire en les vecteurs de $\mathcal{F} \setminus \{\vec{u}_i\}$. On a

$$\begin{aligned}
\vec{v} &= \lambda'_1 \cdot_E \vec{u}_1 +_E \ldots +_E \lambda'_k \cdot_E \vec{u}_k \\
&= \lambda'_1 \cdot_E \vec{u}_1 +_E \ldots +_E \lambda'_{i-1} \cdot_E \vec{u}_{i-1} +_E \lambda'_i \cdot_E \vec{u}_i +_E \lambda'_{i+1} \cdot_E \vec{u}_{i+1} +_E \ldots +_E \lambda'_k \cdot_E \vec{u}_k \\
&= \lambda'_1 \cdot_E \vec{u}_1 +_E \ldots +_E \lambda'_{i-1} \cdot_E \vec{u}_{i-1} +_E \\
&\qquad \lambda'_i \cdot_E (\mu_1 \cdot_E \vec{u}_1 +_E \ldots +_E \mu_{i-1} \cdot_E \vec{u}_{i-1}) +_E \lambda'_{i+1} \cdot_E \vec{u}_{i+1} +_E \ldots +_E \lambda'_k \cdot_E \vec{u}_k \\
&= (\lambda'_1 + \lambda'_i \mu_1) \cdot_E \vec{u}_1 +_E \ldots +_E (\lambda'_{i-1} + \lambda'_i \mu_{i-1}) \cdot_E \vec{u}_{i-1} +_E \lambda'_{i+1} \cdot_E \vec{u}_{i+1} +_E \ldots +_E \lambda'_k \cdot_E \vec{u}_k,
\end{aligned}$$

le dernier terme étant une combinaison linéaire en les vecteurs de $\mathcal{F} \setminus \{\vec{u}_i\}$. □

Corollaire 5.14. *Si $\mathcal{F} = \{\vec{u}_1, ..., \vec{u}_\ell\}$ est une famille génératrice de E avec tous les $\vec{u}_i$ non nuls, on peut extraire une base $\mathcal{B} \subseteq \mathcal{F}$ de E.*

Démonstration. Si $\mathcal{F}$ est libre, on pose $\mathcal{B} = \mathcal{F}$. Sinon, il existe un vecteur $\vec{u}_{i_1}$ tel que $\mathcal{F}_1 = \mathcal{F} \setminus \{\vec{u}_{i_1}\}$ soit encore une famille génératrice de E. Si $\mathcal{F}_1$ est libre, on pose $\mathcal{B} = \mathcal{F}_1$. Sinon, il existe un vecteur $\vec{u}_{i_2}$ tel que $\mathcal{F}_2 = \mathcal{F}_1 \setminus \{\vec{u}_{i_2}\}$ soit encore une famille génératrice de E. On continue ainsi de suite jusqu'à obtenir une famille $\mathcal{F}_i$ libre. On pose alors $\mathcal{B} = \mathcal{F}_i$. □

Théorème 5.15 (dit de la base incomplète)**.** *Soit E un $\mathbb{K}$-esapce vectoriel finiment engerndré. Alors toute famille libre $\mathcal{F}$ de E peut être complétée en un base. De plus si E est engendré par $\vec{u}_1, ..., \vec{u}_n$, on peut compléter $\mathcal{F}$ avec seulement des vecteurs $/vu_i$.*

Démonstration. Soit $\mathcal{F} = \{\vec{v}_1, ..., \vec{v}_k\}$ une famille génératrice de E. Comme $\{\vec{u}_1, ..., \vec{u}_n\}$ est une famille génératrice de E, la famille $\mathcal{F}_0 = \{\vec{v}_1, ..., \vec{v}_k, \vec{u}_1, ..., \vec{u}_k\}$ est une famille génératrice de E. Si $\mathcal{F}_0$ est de plus libre, c'est une base de E. Sinon, par le lemme 5.13, il existe un vecteur de $\mathcal{F}_0'$ qui est linéairement indépendant de ceux qui le précedent. Ce ne peut pas être l'un des $\vec{v}_i$ car $\mathcal{F}$ est libre, c'est donc l'un des $\vec{u}_i$. On construit alors une famille $\mathcal{F}_1$ qui est encore génératrice de E mais un avec un vecteurs $\vec{u}_i$ de moins. En répetant l'argument on trouve une base $\mathcal{F}_j$ de E contenant $\mathcal{F}$ et des $\vec{u}_i$. □

4 Dimension d'un espace vectoriel

Théorème 5.16. *Soit E un $\mathbb{K}$-espace vectoriel finiment engendré, alors toutes les bases de E ont le même nombre de vecteurs.*

Démonstration. Soient $\mathcal{B} = \{\vec{v}_1, ..., \vec{v}_s\}$, $\mathcal{B}' = \{\vec{w}_1, ..., \vec{w}_t\}$deux bases arbitraires de E. Posons $\mathcal{F}_0 = \mathcal{B}'$. La famille $\mathcal{F}_0$ étant génératrice de E, le vecteur $\vec{v}_1$ est combinaison linéaire en les éléments de $\mathcal{F}_0$. La famille $\{\vec{v}_1\} \cup \mathcal{F}_0$ n'est donc pas libre. Par le lemme 5.13, il existe un veteur de $\{\vec{v}_1\} \cup \mathcal{F}_0$ qui est combinaison linéaire de ceux qui le précèdent. Ce ne peut pas être $\vec{v}_1$, c'est donc l'un des $\vec{w}_i$. Quitte à renommer les $\vec{w}_j$, on peut supposer que c'est $\vec{w}_t$. La famille $\mathcal{F}_1 = \{\vec{v}_1, \vec{w}_1, ..., \vec{w}_{t-1}\}$ est encore génératrice. Le vecteur $\vec{v}_2$ est donc combinaison linéaire en les vecteurs de $\mathcal{F}_1$. La famille $\{\vec{v}_2\} \cup \mathcal{F}_1$ n'est donc pas libre et l'un de ses vecteurs s'expriment comme combinaison linéaire en ceux qui le précèdent. Ce ne peut pas être l'un des $\vec{v}_i$ car la famille $\mathcal{B}$ est libre. C'est donc l'un des $\vec{w}_i$. Quitte à renommer les $\vec{w}_j$, on peut supposer que c'est $\vec{w}_{t-2}$. On pose alors $\mathcal{F}_2 = \{\vec{v}_1, \vec{v}_2, \vec{w}_1, ..., \vec{w}_{t-2}\}$.

A la k ème étape, on a $\mathcal{F}_k = \{\vec{v}_1, ..., \vec{v}_k, \vec{w}_1, ..., \vec{w}_{t-k}\}$ qui est une famille génératrice. Si par l'absurde $t < s$ on obtient la famille genératrice $\mathcal{F}_t = \{\vec{v}_1, ..., \vec{v}_t\}$ qui est strictement incluse dans $\mathcal{B}$. Ce qui est impossible car $\mathcal{B}$ est libre. On a donc nécessairement $s \leqslant t$. En recommencant en inversant le role de $\mathcal{B}$ et $\mathcal{B}'$ on montre $t \leqslant s$. On donc montrer $s = t$. □

Définition 5.17. Soit E un $\mathbb{K}$-esapce vectoeirl finiment engendré, la dimension de E est le nombre de vecteurs dans une base de E, on la note $\dim(E)$.

Exemple. La famille $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$ est une base de $\mathbb{R}^3$, qui est donc de dimension 3. Un plan P, avec $\vec{0} \in P$ est un esapce vectoriel de dimension 2. Une droite vectoriel est de dimension 1.

Par convention l'espace nul $\{\vec{0}\}$ est de dimension 0.

Proposition 5.18. *Soit E un $\mathbb{K}$-espace vectoriel de dimension n.*

$i)$ si $\mathcal{F} = \{\vec{u}_1, ..., \vec{u}_k\}$ est une famille génératrice de E alors $k \geqslant n$. De plus $\mathcal{F}$ est une base de E si et seulement si $k = n$.

$ii)$ si $\mathcal{F} = \{\vec{u}_1, ..., \vec{u}_k\}$ est une famille libre de E alors $k \leqslant n$. De plus $\mathcal{F}$ est une base de E si et seulement si $k = n$.

Démonstration. Montrons i). Par le corollaire 5.14, on peut extraire de $\mathcal{F}$ une base $\mathcal{B} \subseteq \mathcal{F}$. On a donc $n = \operatorname{Card} \mathcal{B} \leqslant \operatorname{Card} \mathcal{F} = k$. Suposons qu'on a $k = n$ et montrons que la famille $\mathcal{F}$ est libre. Sinon, par le lemme 5.13, on peut enelever un vecteur de $\mathcal{F}$ et obtenir encore une famille génératrice. On aurait alors, par la première partie du i), $k - 1 \geqslant n$, ce qui est impossible.

Montrons ii). Par le théorème de la base incomplète, on peut ajouter des vecteurs à $\mathcal{F}$ pour obtenir une base $\mathcal{B}$ de E. Ce qui donne $k = \operatorname{Card} \mathcal{F} \leqslant \operatorname{Card} \mathcal{B} = n$. Supposons qu'on a $k = n$ et montrons que la famille $\mathcal{F}$ est génératrice. Sinon, il existe $\vec{u} \in E$ qui ne peut pas s'exprimer comme combinaison linéaire en les vecteurs de $\mathcal{F}$. La famille $\mathcal{F}' = \mathcal{F} \cup \{\vec{u}\}$ serait donc libre. Ce qui, par la première partie du ii) implique $k + 1 \leqslant n$, ce qui n'est pas possible. □

Exemple (de calcul de dimension)**.** Notons E l'espace vectoriel des polynomes sur $\mathbb{R}$ de degré $\leqslant 3$ qui ont 0 et 1 comme racines. Le polynôme $x(x-1)$ divise donc les éléments de E. Comme $P \in E$ est de degré $\leqslant 3$, la seule possiblilté est $P = x(x-1)(bx+a)$. On a donc $P = a(x^2 - x) + b(x^3 - x^2)$. La famille $\{xr - x, x^3 - x^2\}$ est donc une famille génératrice de E. Elle est libre car $\lambda(x^2 - x) + \mu(x^3 - x) = 0$ implique $\lambda = \mu = 0$. On a donc trouvé une base de E à deux éléments et donc $\dim E = 2$.

Corollaire 5.19. *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et F un sous-espace vectoriel de E. Alors on* $\dim(F) \leqslant \dim(E)$ *et $F = E$ si et seulement si* $\dim(F) = \dim(E)$.

Démonstration. Notons n la dimension de E et k celle de F. Soit $\mathcal{B}$ une base de F. La famille $\mathcal{B}$ est donc une famille libre de E. Le nombre de vecteur dans $\mathcal{B}$ étant k on a $k \leqslant n$ par proposition 5.18. De plus ona $E = F$ si et suelement si $\mathcal{B}$ est une base de E donc, toujours par propostion 5.18, si et seulement si $k = n$. □

5 Rang d'une matrice

Lemme 5.20. *L'ensemble $M_{m,n}(\mathbb{K})$ muni de la somme de matrice et le multpication scalaire :*

$$\lambda(a_{i,j}) = (\lambda a_{i,j})$$

est un espace vectoriel.

L'espace $\mathbb{R}^n$ des colonnes de taille n en est un cas particulier : $\mathbb{R}^n = M_{n,1}(\mathbb{R})$. De même pour les lignes de tailels n ($M_{1,n}(\mathbb{R})$)

Définition 5.21. Le *rang* d'une matrice A est la dimension de l'espace vectoriel engendré par les lignes de A

Exemple. Soit la matrice A de $M_{3,5}(\mathbb{R})$ définit par

$$A = \begin{bmatrix} 0 & 1 & 3 & 0 & 4 \\ 0 & 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

L'espace des lignes est

$$E = \text{Vect}_{\mathbb{R}}\left([0,1,3,0,4],[0,0,0,1,5]\right)$$

On a une famille génératrice à 2 vecteurs. Cette famille est aussi libre, c'est donc une base de E. Ce qui donne $\operatorname{rang}(A) = 2$.

Lemme 5.22. *Le rang d'une matrice échelonnée réduite A sur un corps $\mathbb{K}$ est le nombre de lignes non nulles de A.*

Comment calculer le rang d'une matrice arbitraire ?

Définition 5.23. Deux matrice s $A, B \in M_{m,n}(\mathbb{K})$ sont ligne équivalents s'il existe une suite d'opérations élémentaitres de ligne transformant A en B.

Proposition 5.24. *La relation $A\mathcal{R}B \Leftrightarrow A$ est ligne équivalente à B est une relation d'équivalence.*

Démonstration. Réfléxivité : A s'obtient de A en ne faisant qucune opération.

Transitivité : Supposons $A\mathcal{R}B$ et $B\mathcal{R}C$. Notons s_1 la suite d'opérations de lignes élémentaires permettant de passer de A à B et s_2 celle permettant de passer de B à C. Alors la matrice C s'obtient de A en effectuant les opérations de s_1 puis celles de s_2. On a donc bien $A\mathcal{R}C$.

Symétrie : Montrons d'abord que chaque opération élémetaire admet un inverse. Si M' s'obtient de M pa

– $L_i \to L'_j, L_j \to L'_i$ alors M s'obtient de M par $L'_i \to L_j, L'_j \to L_i$
– $cL_i \to L'_i$ avec $c \neq 0$ alors M s'obtient de M' apr $\frac{1}{c}L'_i \to L_i$
– $L_i + cL_j \to L'_i$ alors M s'obtient de M' apr $L'_i - cL'_j \to L_i$

ainsi si B s'obient de A par une suite d'opération s alors A s'obtient de B en effectuant les opérations inverses et dans l'odre inverse à celui de s □

Théorème 5.25. *Deux matrices lignes équivalentes A et B ont exactement le même espace vectoriel engendré par les lignes. En particulier, elles ont le même rang.*

Démonstration. Il suffit de montrer qu'une opération élémentaire de ligne sur A ne change pas l'esapce vectoriel engendré par les lignes de A

$i)$ $L_i \leftrightarrow L_j$. On a bien $\text{Vect}_{\mathbb{K}}(L_1, ..., L_i, ..., L_j, ..., L_m) = \text{Vect}_{\mathbb{K}}(L_1, ..., L_j, ..., L_i, ..., L_m)$.

$ii)$ $L_i \to L'_i = cL_i$ avec $c \not{0}$ Soit $\vec{v} \in \text{Vect}_{\mathbb{K}}(L'_1, ..., L'_m)$. Il existe donc $a_1, ..., a_m$ vérifiant

$$\vec{v} = a_1L'_1 + ... + a_iL'_i + ... + a_mL'_m = a_1L_1 + ... + (ca_i)L_i + ... + a_mL_m$$

On a donc $\vec{v} \in \text{Vect}_{\mathbb{K}}(L_1, ..., L_m)$ puis $\text{Vect}_{\mathbb{K}}(L'_1, ..., L'_m) \subseteq \text{Vect}_{\mathbb{K}}(L_1, ..., L_m)$ Comme $L'_i = cL_i$ implique $L_i = \frac{1}{c}L'_i$, en utilisant un argument symétrique inversant les rôles de L_i et L'_i on obtient $\text{Vect}_{\mathbb{K}}(L_1, ..., L_m) \subseteq \text{Vect}_{\mathbb{K}}(L'_1, ..., L'_m)$.

$iii)$ $L_i \to L'_i = L_i + cL_j$ Soit $\vec{v} \in \text{Vect}_{\mathbb{K}}(L'_1, ..., L'_m)$. Il existe donc $a_1, ..., a_m$ vérifiant

$$\vec{v} = a_1L'_1 + ... + a_iL'_i + ... + a_mL'_m = a_1L_1 + ... + (a_j + ca_i)L_j + ... + a_mL_m$$

On a donc $\vec{v} \in \text{Vect}_{\mathbb{K}}(L_1, ..., L_m)$ puis $\text{Vect}_{\mathbb{K}}(L'_1, ..., L'_m) \subseteq \text{Vect}_{\mathbb{K}}(L_1, ..., L_m)$ Comme $L'_i = L_i + cL_j$ implique $L_i = L'_i - cL'_j$, en utilisant un argument symétrique inversant les rôles de L_i et L'_i on obtient $\text{Vect}_{\mathbb{K}}(L_1, ..., L_m) \subseteq \text{Vect}_{\mathbb{K}}(L'_1, ..., L'_m)$.

□

Corollaire 5.26. *Si une matrice A se réduit en une matrice échelonnée réduite B, alors le rang de A est le nombre de lignes non nulles de B.*

6 Systèmes linéaire homogènes

Définition 5.27. Un système linéaire $AX = B$ est homogène si son second terme B est $\vec{0}$.

Exemple. $A = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & 1-1 \end{bmatrix}$ Le système est $A \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \vec{0}$ soit

$$\begin{cases} x_1 - x_2 = 0 \\ x_2 - x_3 = 0 \end{cases}$$

On a montré les raltions $(A + B) \cdot C = A \cdot C + B \cdot C$ et $C \cdot (A + B) = C \cdot A + C \cdot B$ pour les matrice carrés. Il n'est pas plus difficile de montrer qu'en fait ces relation sont vraies dés que les l'un des membre de ces relation existe.

Lemme 5.28. *Soit $AX = 0$ un système homogène avec $A \in M_{m,n}(\mathbb{K})$, alors*
$i)$ $x_1 = ... = x_n = 0$ est une solution
$ii)$ L'ensemble S des solutions du système est un sous-espace-vectoriel de $\mathbb{K}$.

Démonstration. $i)$ Notons $a_{i,j}$ les coefficient de A On a alors

$$AX = \begin{bmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{bmatrix} \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} a_{1,1} \cdot 0 + ... + a_{1,n} \cdot 0 \\ \vdots \\ a_{m,1} \cdot 0 + ... + a_{m,n} \cdot 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

$ii)$ Si X et Y sont deux solutions (c'est-à-dire $AX = 0$ et $AY = 0$). Alors $A(X + Y) = AX + AY = 0 + 0 = 0$. Si X est une solution et λ un scalaire, alors $A(\lambda X) = \lambda AX = \lambda 0 = 0$. L'ensemble des solutions S est donc un sou-espace vectoriel de $\mathbb{K}^n$. □

Définition 5.29. Soit A une matrice de $M_{m,n}(\mathbb{K})$. L'esapce *zéro* de A, noté $\mathrm{Nul}(A)$ est l'espace vectoriel des solutions du système $AX = 0$.

Proposition 5.30. *Soit $AX = B$ un système linéaire. Soit X_0 une solution de ce système. Alors l'ensemble S des solutions de ce système est*

$$S = \{X_0 + Y \,|\, Y \in \mathrm{Nul}(A)\}$$

Proposition 5.31. *Posons $S' = \{X_0 + Y \,|\, Y \in \mathrm{Nul}(A)\}$. Soit Y un élément de $\mathrm{Nul}(A)$. Alors $A(X_0 + Y) = AX_0 + AY = B + 0 = B$. On a donc $S' \subseteq S$. Montrons $S \subseteq S'$. Soit X une solution. On a $X = X_0 + (X - X_0)$ avec $A(X - X_0) = AX - AX_0 = B - B = 0$ et donc $X - X_0 \in \mathrm{Nul}(A)$. Ce qui donne $S \subseteq S'$. On a donc montré $S = S'$.*

7 Opérations d'espaces vectoriels

Définition 5.32. Soient E un $\mathbb{K}$-espace vectoriel et F, G des sous-espace vectoriels de E. La *somme* de F et G est l'ensemble

$$F + G = \{u + v \,|\, u \in F,\ v \in G\}$$

Exemple. Prenons $E = \mathbb{R}^3$, $F = \mathrm{Vect}_{\mathbb{K}}\left(\begin{bmatrix}1\\0\\0\end{bmatrix}\right)$ l'axe des x et $G = \mathrm{Vect}_{\mathbb{K}}\left(\begin{bmatrix}0\\1\\0\end{bmatrix}\right)$ l'axe des y. Alors la somme $F + G$ est l'ensemble des vecteurs $\lambda\begin{bmatrix}1\\0\\0\end{bmatrix} + \mu\begin{bmatrix}0\\1\\0\end{bmatrix}$ pour $\lambda, \mu \in \mathbb{R}$, c'est à dire le plan (xy).

Proposition 5.33. *Reprenons les notations de la définition 5.32. L'ensemble $F+G$ est un sous-espace vectoriel de E.*

Démonstration. Soient w_1 et w_2 deux éléments de $F + G$. Il existe alors u_1, u_2 dans F et v_1, v_2 dans G tels que $w_1 = u_1 + v_1$ et $w_2 = u_2 + v_2$. On a alors

$$w = w_1 + w_2 = u_1 + v_1 + u_2 + v_2 = u_1 + u_2 + v_1 + v_2 = u + v$$

avec $u = u_1 + u_2 \in F$ et $v = v_1 + v_2 \in G$. Le vecteur $w_1 + w_2$ est donc dans $F + G$. Soit de plus λ un élément de $\mathbb{K}$. Alors on a

$$\lambda w_1 = \lambda(u_1 + v_1) = \lambda u_1 + \lambda u_2$$

Comme λu_1 est dans F et λu_2 est dans G le vecteur λw_1 est dans $F + G$. L'ensemble $F + G$ est donc bien un sous-espace vectoriel de E. $\square$

Proposition 5.34. *Soient E un $\mathbb{K}$-espace vectoriel et F, G des sous-espace vectoriels de E. L'intersection de $F \cap G$ est un sous-espace vectoriel de E.*

Démonstration. Soient u et v deux éléments de $F \cap G$ et λ un élément de $\mathbb{K}$. Comme u et v sont dans $F \cap G$ et donc en particulier dans F qui est un espace vectoriel, on a $u + v \in F$ et $\lambda u \in F$. De même on a $u + v \in G$ et $\lambda u \in G$. Ces relations établissent $u + v \in F \cap G$ et $\lambda u \in F \cap G$. $\square$

Attention, en général la réunion de sous-espace vectoriel n'est pas un espace vectoriel. Prenons $E = \mathbb{R}^2$, F la droite $\mathrm{Vect}_{\mathbb{R}}\left(\begin{bmatrix}1\\0\end{bmatrix}\right)$ et G la droite $\mathrm{Vect}_{\mathbb{R}}\left(\begin{bmatrix}0\\1\end{bmatrix}\right)$. [Faire dessin]

Proposition 5.35. *Soient E un $\mathbb{K}$-espace vectoriel de dimension et F, G deux sous-espaces vectoriel de E. Alors on a*

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

Démonstration. Comme E est de dimension finie, les espaces vectoriels $F, G, F + G$ et $F \cap G$ sont de dimension finies. Soit $\mathcal{B}$ une base de $F \cap G$. La famille $\mathcal{B}$ est une famille libre de F. Par le théorème de la base incomplète il existe des vecteurs $\{u_1, ..., u_p\}$ tels que $\mathcal{B}_F = \mathcal{B} \cup \{u_1, ..., u_p\}$ soit une base de F. On a donc $\dim(F) = \dim(F \cap G) + p$. De même il existe des vecteurs $\{v_1, ..., v_q\}$ tels que $\mathcal{B}_G = \mathcal{B} \cup \{v_1, ..., v_p\}$ soit une base de G et $\dim(G) = \dim(F \cap G) + q$. Montrons que la famille $\mathcal{C} = \mathcal{B} \cup \{u_1, ..., u_p\} \cup \{v_1, ..., v_q\}$ est une base de $F + G$. Soit w un vecteur de $F + G$. Par définition de $F + G$, il existe $u \in F$ et $v \in G$ tels que $w = u + v$. Comme u est dans F, il est combinaison linéaire en les vecteurs de $\mathcal{B}_F$ et donc en les u_i et les vecteurs de $\mathcal{B}$. Comme v est dans G, il est combinaison linéaire en les vecteur de $\mathcal{B}_G$ et donc en les v_i et les vecteurs de $\mathcal{B}$. Le vecteur w qui est égal à $u + v$ est donc combinaison linéaire en les u_i, les v_i est les vecteurs de $\mathcal{B}$, ce qui revient à dire qu'il est combinaison linéaire en les vecteurs de $\mathcal{C}$. La famille $\mathcal{C}$ est donc une famille génératrice de $F+G$. Montrons que c'est une famille libre. Posons $\mathcal{B} = \{w_1, ..., w_r\}$ et soient λ_i pour $i = 1, ..., p$, μ_j pour $j = 1, ..., w$ et η_k pour $k = 1, .., r$ des réels tels que

$$\lambda_1 u_1 + ... + \lambda_p u_p + \mu_1 v_1 + ... + \mu_q v_q + \eta_1 w_1 + ... + \eta_r w_r = 0 \tag{5.1}$$

On a donc

$$\mu_1 v_1 + ... + \mu_q v_q + \eta_1 w_1 + ... + \eta_r w_r = -\lambda_1 u_1 - ... - \lambda_p u_p$$

Notons w ce vecteur. Le membre de gauche est une combinaison linéaire en les vecteurs de $\mathcal{B}_G$ tandis que le membre de droite est dans F. Le vecteur w est donc dans $F \cap G$. Comme $\mathcal{B}$ est une base de $F \cap G$. Il existe des coefficient $\eta'_1, ..., \eta'_r$ tels que $w = \eta' 1 w_1 + ... + \eta'_r w_r$. On a donc

$$\begin{aligned} 0 &= w - w \\ &= \mu_1 v_1 + ... + \mu_q v_q + \eta_1 w_1 + ... + \eta_r w_r - (\eta'_1 w_1 + ... + \eta'_r w_r) \\ &= \mu_1 v_1 + ... + \mu_q v_q + (\eta_1 - \eta'_1) w_1 + ... + (\eta_r - \eta'_r) w_r \end{aligned}$$

La famille $\mathcal{B}_G$ étant une base et donc libre, on a nécessairement $\mu_1 = ... = \mu_q = 0$. La combinaison linéaire (5.1) devient donc

$$\lambda_1 u_1 + ... + \lambda_p u_p + \eta_1 w_1 + ... + \eta_r w_r = 0$$

La famille $\mathcal{B}_F$ étant une base et donc libre, on a $\lambda_1 = ... = \lambda_p = \eta_1 = ... = \eta_r = 0$. La famille $\mathcal{C}$ étant génératrice et libre de $E + F$, c'est une base. On a donc

$$\begin{aligned} \dim(F+G) &= \dim(F \cap G) + p + q \\ &= \dim(F \cap G) + p + \dim(F \cap G) + q - \dim(F \cap G) \\ &= \dim(F) + \dim(G) - \dim(F \cap G). \end{aligned}$$

□

Définition 5.36. Soient E un $\mathbb{K}$-espace vectoriel et F, G deux sous-espaces vectoriels de E. On dit que E est *somme directe* de F et G si

$i)$ $E = F + G$

$ii)$ $F \cap G = \{0\}$

On le note alors par $E = F \oplus G$.

Lemme 5.37. *Soient E un $\mathbb{K}$-espace vectoriel et F, G tels que $E = F \oplus G$. Alors tout vecteur w de E s'écrit de manière unique sous la forme $w = u + v$ avec $u \in F$ et $v \in G$.*

Démonstration. Soit w un vecteur de E. Supposons qu'ils existent u_1, u_2 de F et v_1, v_2 de G tels que $w = u_1 + v_1 = u_2 + v_2$. De $0 = w - w = u_1 + v_1 - u_2 - v_2$ on obtient $u_2 - u_1 = v_1 - v_2$. Le membre de gauche est dans F tandis que celui de droite est dans G. Ainsi $u_1 - u_2 = v_2 - v_1 = 0$ car $F \cap G = \{0\}$. On a donc montré $u_1 = u_2$ et $v_1 = v_2$ et que l'écriture de w est unique. □

Corollaire 5.38. *Soient E un $\mathbb{K}$-espace vectoriel et F, G tels que $E = F \oplus G$. Alors* $\dim(E) = \dim(F) + \dim(G)$.

Démonstration. Par la proposition 5.35, on a $\dim(E) = \dim(F + G) = \dim(F) + \dim(G) - \dim(F \cap G)$. Comme par hypothèse $F \cap G = \{0\}$, on a $\dim(F \cap G) = 0$ et donc $\dim(E) = \dim(F) + \dim(G)$. □

Lemme 5.39. *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Alors pour tout sous-espace vectoriel F de E, il existe un sous-espace vectoriel G de E tel que $E = F \oplus G$.*

L'espace vectoriel G est le *supplémentaire* de F dans G.

Démonstration. Soit $\mathcal{B} = (u_1, ..., u_p)$ une base de F. Par le théorème de la base incomplète on peut lui ajouter $\mathcal{C} = (v_1, ..., v_q)$ tels que $\mathcal{B} \cup \mathcal{C}$ soit une base de E. Posons $F = \mathrm{Vect}_{\mathbb{K}}(\mathcal{C})$. Montrons $E = F \oplus G$. Montrons d'abord $E = F + G$. Soit w un vecteur de E. Comme $\mathcal{B} \cup \mathcal{C}$ est une base de E, il existe des coefficients $\lambda_1, ..., \lambda_p$ et $\mu_1, ..., \mu_q$ tels que

$$w = \lambda_1 u_1 + ... + \lambda_p u_p + \mu_1 v_1 + ... + \mu_q v_q$$

Posons $u = \lambda_1 u_1 + ... + \lambda_p u_p$ et $v = \mu_1 v_1 + ... + \mu_q v_q$. Le vecteur u étant dans F tandis que v est dans G, on a $w \in F + G$ et donc $E = F + G$. Montrons maintenant $F \cap G = \{0\}$. Soit w un vecteur de $F \cap G$. Comme w est dans F, il existe $\lambda_1, ..., \lambda_p$ tels que $w = \lambda_1 u_1 + ... + \lambda_p u_p$. De même, comme w est dans G, il existe $\mu_1, ..., \mu_p$ tels que $w = \mu_1 v_1 + ... + \mu_q v_q$. On a donc

$$0 = w - w = \lambda_1 u_1 + ... + \lambda_p u_p - \mu_1 v_1 - ... - \mu_q v_q$$

La famille $\mathcal{B} \cup \mathcal{C}$ étant une base, et donc libre, on a $\lambda_1 = ... = \lambda_p = \mu_1 = ... = \mu_q = 0$. Il s'en suit $w = 0$ et donc $F \cap G = \{0\}$. $\square$

VI. Applications linéaires

1 Notions de base

Définition 6.1. Soient E, F deux $\mathbb{K}$-espaces vectoriels. Une application linéaire $\phi = E \to F$ est une application vérifiant

– pour tout u, v de E, $\phi(u +_E v) = \phi(u) +_F \phi(v)$,
– pour tout u de E et tout λ de $\mathbb{K}$, $\phi(\lambda \cdot_{\mathbb{K}} u) = \lambda \cdot_{\mathbb{K}} \phi(v)$.

Exemple.

1) Prenons $E = F = \mathbb{R}^2$. La symétrie centrale

$$\begin{array}{rcl} \phi : E & \to & F \\ \begin{bmatrix} x \\ y \end{bmatrix} & \mapsto & \begin{bmatrix} -x \\ -y \end{bmatrix} \end{array}$$

est une application linéaire.

2) Prenons $E = \mathbb{R}[X]_{\leqslant n}$ les polynômes sur $\mathbb{R}$ de degré $\leqslant n$ et $F = \mathbb{R}[X]_{\leqslant n-1}$. La fonction ϕ de E dans F qui à P associé P' est une application linéaire.

3)La translation de vecteur w

$$\begin{array}{rcl} t_w : E & \to & E \\ v & \mapsto & v + w \end{array}$$

n'est pas une application linéaire. En effet pour u, v de E, on a $t_w(u + v) = u + v + w$ tandis que $t_w(u) + t_w(v) = u + w + v + w$.

Proposition 6.2. *Soient E et F deux $\mathbb{K}$-espace vectoriels et ϕ une application linéaire de E dans F, alors*

$i)$ $\phi(0_E) = 0_F$

$ii)$ Si $u = \lambda_1 u_1 + ... + \lambda_n u_n$ avec $\lambda_i \in \mathbb{K}$ et $u_i \in E$, alors

$$\phi(u) = \lambda_1 \phi(u_1) + ... + \lambda_n \phi(u_n)$$

Démonstration. Montrons $i)$. On a $0_E = 0_E + 0_E$, d'où $\phi(0_E) = \phi(0_E) + \phi(0_E)$ et donc $0_F = \phi(0_E)$. Montons $ii)$ par récurrence sur n. Le résultat est vraie pour $n = 2$ par définition d'une application linéaire. Supposons le résultat vrai au rang $n - 1$ et montrons le au rang n. On a

$$\begin{aligned} \phi(\lambda_1 u_1 + ... + \lambda_n u_n) &= \phi((\lambda_1 u_1 + ... + \lambda_{n-1} u_{n-1}) + \lambda_n u_n) \\ &= \phi(\lambda_1 u_1 + ... + \lambda_{n-1} u_{n-1}) + \phi(\lambda_n u_n) \\ &= \phi(\lambda_1 u_1 + ... + \lambda_{n-1} u_{n-1}) + \lambda_n \phi(u_n) \\ &= \lambda_1 \phi(u_1) + ... + \lambda_{n-1} \phi(u_{n-1}) + \lambda_n \phi(u_n) \end{aligned}$$

□

Définition 6.3. Soient E et F deux $\mathbb{K}$-espaces vectoriels et ϕ une application linéaire de E dans F.

$i)$ le noyau de ϕ est le sous-ensemble $\ker(\phi)$ de E définie par

$$\ker(\phi) = \{u \in E \,|\, \phi(u) = 0\}$$

$ii)$ l'image de ϕ est le sous-ensemble $\mathrm{Im}\,\phi)$ de F définie par

$$\mathrm{Im}(\phi) = \{v \in F \,|\, \exists u \in E \text{ avec } \phi(u) = v\}$$

Proposition 6.4. *Avec les notations de la définition 6.3 on a*

$i)$ $\ker(\phi)$ *est un sous-espace vectoriel de* E

$ii)$ $\mathrm{Im}(\phi)$ *est un sous-espace vectoriel de* F

Démonstration. Montrons $i)$. Soient u_1 et u_2 deux éléments de $\ker(\phi)$. On a $\phi(u_1 + u_2) = \phi(u_1) + \phi(u_2)$. Comme u_1 et u_2 sont dans $\ker(\phi)$, on a $\phi(u_1) = \phi(u_2) = 0_F$. On en déduit $\phi(u_1 + u_2) = 0_F$ et donc $u_1 + u_2 \in \ker(\phi)$. Soient $\lambda \in \mathbb{K}$ et $u \in \ker(\phi)$. On a $\phi(\lambda u) = \lambda \cdot \phi(u) = \lambda \cdot 0_F = 0_F$. On a donc $\lambda u \in \ker(\phi)$. Le sous-ensemble $\ker(\phi)$ de E est donc un sous-espace vectoriel de E.

Montrons $ii)$. Soient v_1 et v_2 deux éléments de $\mathrm{Im}(phi)$ et λ dans $\mathbb{K}$.. Par définition de $\mathrm{Im}(\phi)$, il existe u_1 et u_2 dans E tels que $\phi(u_1) = v_1$ et $\phi(u_2) = v_2$. On a donc $v_1 + v_2 = \phi(u_1) + \phi(u_2) = \phi(u_1 + u_2)$, ce qui établit $v_1 + v_2 \in \mathrm{Im}(\phi)$. On a aussi $\lambda v_1 = \lambda\phi(u_1) = \phi(\lambda u_1)$ et donc $\lambda v_1 \in \mathrm{Im}(\phi)$. Le sous-ensemble $\mathrm{Im}(\phi)$ de F est donc un sous-espace vectoriel de F. $\square$

Exemple. Prenons $E = F = \mathbb{R}^3$. On note ϕ la projection sur le plan (XY) parallèlement à l'axe z. Pour tout x, y, z de $\mathbb{R}^3$, on a $\phi\left(\begin{bmatrix} x \\ y \\ z \end{bmatrix}\right) = \begin{bmatrix} x \\ y \\ 0 \end{bmatrix}$.

- $\ker(\phi)$ est l'axe des z, c'est-à dire l'espace vectoriel $\mathrm{Vect}_{\mathbb{K}}\left(\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}\right)$.

- $\mathrm{Im}(\phi)$ est le plan (XY), c'est-à-dire l'espace vectoriel $\mathrm{Vect}_{\mathbb{K}}\left(\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}\right)$. On remarque $\dim\ker(\phi) = 1$ et $\dim\mathrm{Im}\,\phi = 3$. L'addition des deux donne 3 qui est la dimension de $\mathbb{R}^3$.

2 Théorème du rang

Lemme 6.5. *Soient E et F deux $\mathbb{K}$ espace vectoriels, avec E de dimension finie, et ϕ une application linéaire de E sur F. Si de plus $\mathcal{B} = (u_1, ..., u_n)$ est une base de E, alors on a* $\mathrm{Im}(\phi) = \mathit{Vect}_{\mathbb{K}}\,(\phi(u_1), ..., \phi(u_n))$.

Démonstration. Comme $\mathrm{Im}(\phi)$ est un sous-espace vectoriel de F et que $\phi(u_1), ..., \phi(u_n)$ sont dans ϕ. On a

$$\mathrm{Vect}_{\mathbb{K}}\,(\phi(u_1), ..., \phi(u_n)) \subseteq \mathrm{Im}(\phi).$$

Montrons qu'il y a égalité. Soit v un vecteur de $\mathrm{Im}(\phi)$ arbitraire. Il existe u dans E tel que $v = \phi(u)$. Comme $\mathcal{B}$ est une base de E, il existe des scalaires $\lambda_1, ..., \lambda_n$ tels que $u = \lambda_1 u_1 + ... + \lambda_n u_n$. On a donc

$$v = \phi(u) = \phi(\lambda_1 u_1 + ... + \lambda_n u_n) = \lambda_1\phi(u_1) + ... + \lambda_n\phi(u_n)$$

qui appartient à $\mathrm{Vect}_{\mathbb{K}}\,(\phi(u_1), ..., \phi(u_n))$. $\square$

Théorème 6.6. *Soient E et F deux $\mathbb{K}$-espace vectoriels et $\phi : E \to F$ une application linéaire. On suppose de plus que E est de dimension finie. Alors on a*

$$\dim(E) = \dim(\ker(\phi)) + \dim(\mathrm{Im}(\phi)).$$

Démonstration. Posons $F = \ker(\phi)$. Soit $\mathcal{B} = (u_1, ..., u_p)$ une base de E. On complète $\mathcal{B}$ avec $\mathcal{C} = (v_1, ..., v_q)$ de manière à obtenir une base de E. On pose $G = \mathrm{Vect}_{\mathbb{K}}(\mathcal{C})$. Par le lemme V.5.39, ou plus précisément sa démonstration, on a $E = F \oplus G$. Par le lemme 6.5, on a

$$\mathrm{Im}(\phi) = \mathrm{Vect}_{\mathbb{K}}(\phi(u_1), ..., \phi(u_p), \phi(v_1), ..., \phi(v_q))$$

Comme pour $i = 1, ..., p$, le vecteur u_i est dans $\ker(\phi)$, on a $\phi(u_i) = 0$ et donc $\mathrm{Im}(\phi) = \mathrm{Vect}_{\mathbb{K}}(\phi(v_1), ..., \phi(v_q))$. Montrons que la famille $\mathcal{D} = (\phi(v_1), ..., \phi(v_q))$ est libre. Soient $\lambda_1, ..., \lambda_n$ tels que $\lambda_1\phi(v_1) + ... + \lambda_q\phi(v_q) = 0$. Comme ϕ est une application linéaire, on a $\phi(\lambda_1 v_1 + ... + \lambda_q v_q) = 0$ et donc $v = \lambda_1 v_1 + ... + \lambda_q v_q$ appartient à $\ker(\phi)$. D'autre part v appartient à G. On a donc $v \in F \cap G = \{0\}$. Ceci implique $\lambda_1 v_1 + ... + \lambda_q v_q = 0$. Comme $\mathcal{C}$ est une base, donc une famille libre, on a $\lambda_1 = ... = \lambda_q = 0$.

Calculons les dimensions. Comme $E = F \oplus G$, on a $\dim(E) = \dim(F) + \dim(G)$. Or $F = \ker(\phi)$ et $\dim(G) = q = \dim \mathrm{Im}(\phi)$. On a donc montré

$$\dim(E) = \dim(\ker(\phi)) + \dim(\mathrm{Im}(\phi)).$$

□

Définition 6.7. Soit $\phi : E \to F$ une application linéaire. Le *rang* de ϕ est $\dim(\mathrm{Im}(\phi))$.

Lemme 6.8. *Une application linéaire $\phi : E \to F$ est injective si et seulement si* $\ker(\phi) = \{0\}$.

Démonstration. Supposons que ϕ soit injective. Soit u un élément de $\ker(\phi)$. Alors on a $\phi(v) = 0$. Comme on a aussi $\phi(0) = 0$, l'injectivité de ϕ implique $u = 0$ et donc $\ker(\phi) = \{0\}$. Supposons maintenant $\ker(\phi) = \{0\}$ et montrons que ϕ est injective. Soient u et v deux vecteurs de E tels que $\phi(u) = \phi(v)$. Comme ϕ est linéaire, on a $\phi(u-v) = 0$ et donc $u-v$ est un élément de $\ker(\phi)$. L'ensemble $\ker(\phi)$ ne contenant que 0, on a $u - v = 0$ et donc $u = v$. □

Définition 6.9. Soit E un $\mathbb{K}$-espace vectoriel. Une application linéaire de E dans lui même est un *endomorphisme* de E.

Proposition 6.10. *Soit ϕ un endomorphisme d'un $\mathbb{K}$-espace vectoriel E de dimension finie. Alors les assertions suivantes sont équivalentes :*

i) ϕ est injective ;
ii) ϕ est surjective ;
iii) ϕ est bijective ;
iv) ϕ est de rang $\dim(E)$.

Démonstration. Montrons que i) implique ii). Comme ϕ est injective, $\ker(\phi)$ est $\{0\}$ et donc $\dim(\ker(\phi)) = 0$. La théorème du rang implique alors $\dim(\mathrm{Im}(\phi)) = \dim(E)$. D'ou $\mathrm{Im}(\phi) = E$, car $\mathrm{Im}(\phi) \subseteq E$ puis la surjectivité de ϕ.

Montrons que ii) implique iii). Si ϕ est surjective alors $\mathrm{Im}(\phi) = E$ et $\dim(\mathrm{Im}(\phi)) = \dim(E)$. Le théorème du rang implique donc $\dim(\ker(\phi)) = 0$, à savoir $\ker(\phi) = \{0\}$. L'application ϕ est donc injective. Une application surjective et injective est bijective.

Montrons que iii) implique iv). Soit ϕ une application bijective. Comme ϕ est en particulier surjective, on a $\mathrm{Im}(\phi) = E$ et donc $\mathrm{rang}(\phi) = \dim(\mathrm{Im}(\phi)) = \dim(E)$.

Montrons que iv) implique i). Si $\mathrm{rang}(\phi) = \dim(E)$ alors $\dim(\mathrm{Im}(\phi)) = \dim E$ et le théorème du rang implique $\dim(\ker(\phi)) = 0$, ce qui implique $\ker(\phi) = \{0\}$. L'application ϕ est donc injective. □

3 Représentation par rapport à une base

Soit E un $\mathbb{K}$-esapce vectoriel de dimension n. Fixons une base $\mathcal{B} = (u_1, ..., u_n)$ de E.

Un vecteur u s'exprime alors de manière unique comme combinaison linéaire en les vecteurs de $\mathcal{B}$.

$$u = \lambda_1 u_1 + ... + \lambda_n u_n$$

Définition 6.11. Les coordonnées de $u \in E$ par rapport à $\mathcal{B}$ sont

$$\operatorname{coord}_{\mathcal{B}}(u) = \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{bmatrix}$$

Exemple. Prenosn $E = \mathbb{R}[X]_{\leqslant 2}$. Calculer les corrdonnées de $Q(X) = X$ par rapport à la base $\mathcal{B} = (P_1(x), P_2(X), P_3(X))$ avec $P_1(X) = X^2+X+1$, $P_2(X) = X^2-1$ et $P_3(X) = X^2+2X$. On cherche λ_1, λ_2 et λ_3 des réels tels que $Q(X) = \lambda_1 P_1(X) + \lambda_2 P_2(X) + \lambda_3 P_3(X)$. On obtient $X = (\lambda_1 + \lambda_2 + \lambda_3)X^2 + (\lambda_1 + 2\lambda_3)X + \lambda_1 - \lambda_2$. En identifiant les coefficients on trouve $\lambda_1 = -\frac{1}{3} = \lambda_2$ et $\lambda_3 = \frac{2}{3}$. On a donc

$$\operatorname{coord}_{\mathcal{B}}(Q(X)) = \begin{bmatrix} -\frac{1}{3} \\ -\frac{1}{3} \\ \frac{2}{3} \end{bmatrix}$$

Proposition 6.12. *L'application*

$$\begin{array}{rcl} \psi : E & \to & \mathbb{K}^n \\ v & \mapsto & \operatorname{coord}_{\mathcal{B}}(v) \end{array}$$

est une apllication linéaire bijective.

L'application ψ sert à traduire de manière exacte E ne $\mathbb{K}^n$ à l'aide de la base $\mathcal{B}$.

Démonstration. Montrons d'abord que ψ est linéaire. Soient u et v deux vecteurs de E et λ un élément de $\mathbb{K}$. Posons

$$\operatorname{coord}_{\mathcal{B}}(u) = \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{bmatrix} \quad \text{et} \quad \operatorname{coord}_{\mathcal{B}}(v) = \begin{bmatrix} \mu_1 \\ \vdots \\ \mu_n \end{bmatrix}$$

On a alors $u = \lambda_1 u_1 + ... + \lambda_n u_n$ et $v = \mu_1 u_1 + ... + \mu_n u_n$, d'où

$$u + v = (\lambda_1 + \mu_1)u_1 + ... + (\lambda_n + \mu_n)u_n \quad \text{et} \quad \lambda u = (\lambda\lambda_1)u_1 + ... + (\lambda\lambda_n)u_n$$

Ce qui implique

$$\psi(u+v) = \operatorname{coord}_{\mathcal{B}}(u+v) = \begin{bmatrix} \lambda_1 + \mu_1 \\ \vdots \\ \lambda_n + \mu_n \end{bmatrix} = \operatorname{coord}_{\mathcal{B}}(u) + \operatorname{coord}_{\mathcal{B}}(v) = \psi(u) + \psi(v)$$

ainsi que

$$\psi(\lambda u) = \mathrm{coord}_{\mathcal{B}}(\lambda u) = \begin{bmatrix} \lambda\lambda_1 \\ \vdots \\ \lambda\lambda_n \end{bmatrix} = \lambda\,\mathrm{coord}_{\mathcal{B}}(u) = \lambda\psi(u).$$

Montrons que ϕ est bijective. Par la proposition 6.10 il est suffisant de montrer que ψ est invective. Soit u un vecteur de E tels que $\phi(u) = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$. On a donc $u = 0u_1 + ... + 0u_n = 0$, ce qui implique $\ker(\phi) = \{0\}$ et donc la bijectivité de ψ. $\square$

Soient $\phi : E \to F$ une application linéaire avec E de dimension finie. Si $(u_1, ..., u_n)$ est une base de E alors ϕ est entièrement déterminer par $\phi(u_1), ..., \phi(u_n)$. En effet pour tout u de E il existe des scalaires $\lambda_1, ..., \lambda_n$ tels que $u = \lambda_1 u_1 + ... + \lambda_n u_n$ et alors $\phi(u) = \lambda_1\phi(u_1) + ... + \lambda_n\phi(u_n)$.

Définition 6.13. Soient E et F deux $\mathbb{K}$ espace vectoriels de dimension finie. Soient $\mathcal{B} = (u_1, ..., u_n)$ une base de E et $\mathcal{C} = (v_1, ..., v_m)$ une base de F. Pour toute application linéaire $\phi : E \to F$, la matrice de ϕ par rapport aux bases $\mathcal{B}$, notée $\mathrm{mat}_{\mathcal{B},\mathcal{C}}(\phi)$ est la matrice de taille $m \times n$ dont les vecteurs colonnes $c_1, ..., c_n$ sont définis apr $c_i = \mathrm{coord}_{\mathcal{C}}(\phi(u_i)$ pour $i = 1, ..., n$.

Exemple. Prenons $E = \mathbb{R}^3$ et $F = \mathbb{R}^4$. Posons $\mathcal{B} = (e_1, e_2, e_3)$ la base cononique de E et $\mathcal{C} = (f_1, f_2, f_3, f_4)$ la base canonique de F. On considère ϕ l'application linéaire de E dans F définie par $\phi(e_1) = f_1 + f_2$, $\phi(e_2) = -f_1 + f_2 + 2f_3 + f_4$. et $\phi(e_3) = f_1 - f_3 + f_4$/ On a alors

$$\mathrm{mat}_{\mathcal{B},\mathcal{C}}(\phi) = \begin{bmatrix} 1 & -1 & 1 \\ 1 & 1 & 0 \\ 0 & 2 & -1 \\ 0 & 1 & 1 \end{bmatrix}$$

Proposition 6.14. *On conserve les notations de la définition 6.13. Soit u un élément de E. Posons $A = \mathrm{mat}_{\mathcal{B},\mathcal{C}}(\phi)$, $x = \mathrm{coord}_{\mathcal{B}}(c)$ et $y = \mathrm{coord}_{\mathcal{C}}(\phi(u))$. On a alors $y = A \times x$.*

Démonstration. Posons $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ et

$$A = \begin{bmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{bmatrix}$$

On a alors

$$\begin{aligned} A \times x &= \begin{bmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{bmatrix} \times \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{1,1}x_1 + ... + a_{1,n}x_n \\ \vdots \\ a_{n,1}x_1 + ... + a_{n,n}x_n \end{bmatrix} \\ &= x_1 \begin{bmatrix} a_{1,1} \\ \vdots \\ a_{n,1} \end{bmatrix} + ... + x_n \begin{bmatrix} a_{1,n} \\ \vdots \\ a_{n,n} \end{bmatrix} = x_1\,\mathrm{coord}_{\mathcal{C}}(\phi(u_1)) + ... + x_n\,\mathrm{coord}_{\mathcal{C}}(\phi(u_n)) \\ &= \mathrm{coord}_{\mathcal{C}}(x_1\phi(u_1) + ... + x_n\phi(u_n)) = \mathrm{coord}_{\mathcal{C}}(\phi(u)) = y \end{aligned}$$

□

Définition 6.15. Soient E et F deux $\mathbb{K}$-espaces vectoriels on note $\mathcal{L}(E,F)$ l'ensemble des applications linéaires de E dans F.

Théorème 6.16. *Soient E et F deux $\mathbb{K}$-espace vectoriels de dimensions finies respectives n et m. Soient $\mathcal{B}$ une base de E et $\mathcal{C}$ une base de F. L'application*

$$\begin{array}{rcl} \mathrm{mat}_{\mathcal{B},\mathcal{C}} : \mathcal{L}(E,F) & \to & M_{m,n}(\mathbb{K}) \\ \phi & \mapsto & \mathrm{mat}_{\mathcal{B},\mathcal{C}}(\phi) \end{array}$$

est une application bijective.

Démonstration. Montrons que $\mathrm{mat}_{\mathcal{B},\mathcal{C}}$ est une application injective. Soient ϕ et ϕ' dans $\mathcal{L}(E,F)$ tels que $A = \mathrm{mat}_{\mathcal{B},\mathcal{C}}(\phi) = \mathcal{B},\mathcal{C}(\phi')$. Soit u un vecteur de u quelconque et notons x les coordonnées de u dans la base $\mathcal{B}$. Alors les coordonnées de $\phi(u)$ dans la base $\mathcal{C}$ est $A.x$. De même les coordonnées de $\phi'(u)$ dans la base $\mathcal{C}$ sont $A.x$. Il en suit que $\phi(u)$ est égale à $\phi'(u)$ quelque soit u dans E. Les application ϕ et ϕ' sont donc égales et $\mathrm{mat}_{\mathcal{B},\mathcal{C}}$ est injective.

Montrons que $\mathrm{mat}_{\mathcal{B},\mathcal{C}}$ est une application surjective. Soit A une matrice de $M_{m,n}(\mathbb{K})$. On note $(a_{i,j})$ les coefficients de A. Posons $w_i = a_{1,i}v_1 + ... + a_{m,i}v_m$, qui est un vecteur de F, pour $i = 1, ..., n$. On définit une application $\phi : E \to F$ par

$$\phi(\lambda_1 u_1 + ... + \lambda_n u_n) = \lambda_1 w_1 + ... + \lambda_n w_n.$$

Par construction, l'application ϕ est linéaire. Montrons qu'on a $\mathrm{mat}_{\mathcal{B},\mathcal{C}}(\phi) = A$. Par définition, la i ème colonne de $\mathrm{mat}_{\mathcal{B},\mathcal{C}}(\phi)$ est $c_i = \mathrm{coord}_{\mathcal{C}}(\phi(u_i))$. Or $\phi(u_i) = w_i = a_{1,i}v_1 + ... + a_{m,i}v_m$ et donc $c_i = \begin{bmatrix} a_{1,i} \\ \vdots \\ a_{n,i} \end{bmatrix}$, qui n'est autre que la i ème colonne de A. □

Proposition 6.17. *Soient E, F et G trois espaces vectoriels de dimension finie. Soient $\mathcal{B}$, $\mathcal{C}$ et $\mathcal{D}$ des bases respectives de E, F et G. Soient deux plus $\phi : E \to F$ et $\psi : F \to G$ deux applications linéaires Alors on a*

$$\mathrm{mat}_{\mathcal{B},\mathcal{D}}(\psi \circ \phi) = \mathrm{mat}_{\mathcal{C},\mathcal{D}}(\psi) \times \mathrm{mat}_{\mathcal{B},\mathcal{C}}(\phi)$$

Démonstration. Posons $A = \mathrm{mat}_{\mathcal{B},\mathcal{C}}(\phi)$, $B = \mathrm{mat}_{\mathcal{C},\mathcal{D}}(\psi)$ et $C = \mathrm{mat}_{\mathcal{B},\mathcal{D}}(\psi \circ \phi)$. Soit u un élément de E alors $\mathrm{coord}_{\mathcal{D}}((\psi \circ \phi)(u)) = C\,\mathrm{coord}_{\mathcal{B}}(u)$. Par ailleurs on a $(\psi \circ \phi)(u) = \psi(\phi(u))$ ainsi que $\mathrm{coord}_{\mathcal{C}}(\phi(u)) = A\,\mathrm{coord}_{\mathcal{B}}(u)$ et $\mathrm{coord}_{\mathcal{D}}(\psi(\phi(u))) = B\,\mathrm{coord}_{\mathcal{C}}(\phi(u))$. On a donc $\mathrm{coord}_{\mathcal{D}}(\psi(\phi(u))) = B \times A \times \mathrm{coord}_{\mathcal{C}}(\phi(u))$. Ce qui montre $C = B \times A$. □

Soient E et F deux $\mathbb{K}$-espace vectoriels de dimension respectives n et m. On note $\mathcal{B} = (u_1, ..., u_n)$ une base de E et $\mathcal{C} = (v_1, ..., v_n)$ une base de F. Le tableau suivant dresse les liens entre les notions algébrique et leur traduction par rapport aux bases $\mathcal{B}$ et $\mathcal{C}$.

notion algébrique	traduction par rapport aux bases $\mathcal{B}$ et $\mathcal{C}$
E	$\mathbb{K}^n$
F	$\mathbb{K}^m$
$\phi \in \mathcal{L}(E,F)$	$A \in M_{m,n}(\mathbb{K})$
$\ker(\phi)$	$\mathrm{Nul}(A)$
$\mathrm{Im}(\phi)$	ev engendré par les colonnes de A
$\mathrm{rang}(\phi)$	$\mathrm{rang}(A)$
ϕ bijective	A inversible

4 Changement de base

Définition 6.18. Soit E un espace vectoriel de dimension n et $\mathcal{B} = (u_1, ..., u_n)$ et $\mathcal{C} = (v_1, ..., v_n)$ deux bases de E. La matrice de passage de $\mathcal{B}$ à $\mathcal{C}$ est la matrice P dont les colonnes sont $c_i = \mathrm{coord}_{\mathcal{B}}(w_i)$.

Proposition 6.19. *On conserve les notations de la définition 6.18. Pour tout vecteur u de E, on a* $\mathrm{coord}_{\mathcal{B}}(u) = P\,\mathrm{coord}_{\mathcal{C}}(u)$.

Démonstration. Posons $P = (p_{i,j})$. Par construction de P, on a $v_j = p_{1,j}u_1 + ... + p_{n,j}u_n$ pour tout $j = 1, ..., n$. Soit u un vecteur de E. Posons

$$x = \mathrm{coord}_{\mathcal{B}}(u) = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \quad \text{et} \quad y = \mathrm{coord}_{\mathcal{C}}(u) = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}.$$

On a donc

$$\begin{aligned} v &= y_1v_1 + ... + y_nv_n = y_1(p_{1,1}u_1 + ... + p_{n,1}u_n) + ... + y_n(p_{1,n}u_1 + ... + p_{n,n}u_n) \\ &= (y_1p_{1,1} + ... + y_np_{1,n})u_1 + ... + (y_1p_{n,1} + ... + y_np_{n,n})u_n \end{aligned}$$

Le coefficient devant u_i est $\sum_{k=1}^{n} p_{i,k}y_k$, qui correspond exactement à la loi de produit matrice $P \times$ vecteur y. On a donc bien $x = P \times y$. □

Lemme 6.20. *On conserve les notations de la définition 6.18. La matrice P de changement de base est inversible.*

Démonstration. P est la matrice, par rapport à la base $\mathcal{B}$ de E de l'application linéaire ϕ définie par $\phi(u_i) = v_i$. Comme $\mathrm{Im}(\phi)$ contient tout les v_i et donc la base $\mathcal{C}$. L'application ϕ est donc surjective et donc de $\mathrm{rang}(n)$ par la proposition 6.10. Le rang de P est donc n. Il en suit que P est inversible. □

Théorème 6.21. *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie, $\mathcal{B}$ et $\mathcal{C}$ deux bases de E, P la matrice de passage de la base $\mathbb{B}$ à la base $\mathbb{C}$ et ϕ un endomorphisme de E. Alors on a* $\mathrm{mat}_{\mathcal{C},\mathcal{C}}(\phi) = P^{-1} \times \mathrm{mat}_{\mathcal{B},\mathcal{B}}(\phi) \times P$.

Démonstration. Soit u un élément de E. Par la proposition 6.19 on a $\mathrm{coord}_{\mathcal{B}}(u) = P\,\mathrm{coord}_{\mathcal{C}}(u)$ et $\mathrm{coord}_{\mathcal{B}}(\phi(u)) = P\,\mathrm{coord}_{\mathcal{C}}(\phi(u))$. Par la proposition 6.14 on a

$$\mathrm{coord}_{\mathcal{B}}(\phi(u)) = \mathrm{mat}_{\mathcal{B},\mathcal{B}} \times \mathrm{coord}_{\mathcal{B}}(u) \text{ et } \mathrm{coord}_{\mathcal{C}}(\phi(u)) = \mathrm{mat}_{\mathcal{C},\mathcal{C}} \times \mathrm{coord}_{\mathcal{C}}(u)$$

D'où

$$P\,\mathrm{coord}_{\mathcal{C}}(\phi(u)) = \mathrm{mat}_{\mathcal{B},\mathcal{B}} \times P\,\mathrm{coord}_{\mathcal{C}}(u)$$

et donc

$$\mathrm{coord}_{\mathcal{C}}(\phi(u)) = P^{-1} \times \mathrm{mat}_{\mathcal{B},\mathcal{B}} \times P \times \mathrm{coord}_{\mathcal{C}}(u) = \mathrm{mat}_{\mathcal{C},\mathcal{C}} \times \mathrm{coord}_{\mathcal{C}}(u),$$

ce qui établit $P^{-1} \times \mathrm{mat}_{\mathcal{B},\mathcal{B}} \times P = \mathrm{mat}_{\mathcal{C},\mathcal{C}}$. □

VII. Déterminant

1 Définition du déterminant

Définition 7.1. Soit $n \geqslant 2$. On dit qu'une application

$$\delta : \underbrace{\mathbb{K}^n \times ... \times \mathbb{K}^n}_{n \text{ fois}} \to \mathbb{K}$$

$i)$ est multilinéaire, si on a linéarité en chaque position $i = 1, 2, ..., n$:

$$\delta(u_1, ..., u_{i-1}, u_i + v_i, u_{i+1}, ..., u_n) = \delta(u_1, ..., u_i, ..., u_n) + \delta(v_1, ..., v_i, ..., v_n)$$
$$\delta(u_1, ..., u_{i-1}, \lambda u_i, u_{i+1}, ..., u_n) = \lambda \delta(u_1, ..., u_i, ..., u_n)$$

$ii)$ est alternée, si pour tout $i = 2, ..., n$ on a

$$\delta(u_1, ..., u_i, u_{i+1}, ..., u_n) = -\delta(u_1, ..., u_{i+1}, u_i, ..., u_n)$$

$iii)$ est normalisée dans la base canonique $(e_1, ..., e_n)$ si $\delta(e_1, ..., e_n) = 1$.

Théorème 7.2. *Il existe une et une seule application δ vérifiant $i)$, $ii)$ et $iii)$.*

Définition 7.3. L'unique fonction multilinéaire alternée et normalisée dans la base canonique est appelée *déterminant*. Le déterminant de n vecteurs $u_1, ..., u_n$ de $\mathbb{K}^n$ est noté $\det(u_1, ..., u_n)$. Soit A une matrice carré de $M_n(\mathbb{K})$. Le déterminant de A, noté $\det(A)$ est $\det(c_1, ..., c_n)$ où c_i est le i ème vecteur colonne de A.

Le déterminant d'une matrice A sera notée

$$\det(A) = \begin{vmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{vmatrix}$$

Exemple. Le déterminant d'une matrice $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ est $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$.

Lemme 7.4. *Soit $u_1, ..., u_n$ des vecteurs de $\mathbb{K}^n$. Si deux de ces vecteurs sont égaux alors on a* $\det(u_1, ..., u_n) = 0$.

Démonstration. Soient $i < j$ deux entiers tels que $u_i = u_j$. Par $j - i - 1$ échanges de voisin successifs, on peut supposer $j = i + 1$. On a

$$\begin{aligned} \det(u_1, ..., u_i, u_{i+1}, ..., u_n) &= -\det(u_1, ..., u_{i+1}, u_i, ..., u_n) && \text{car le déterminant est alternée} \\ &= -\det(u_1, ..., u_i, u_{i+1}, ..., u_n) && \text{car } u_i = u_{i+1} \end{aligned}$$

□

2 Calcul du déterminant

Définition 7.5. Soit A une matrice carré de taille n. Notons $A_{i,j}$ la matrice de taille $(n-1) \times (n-1)$ obtenue de A en enlevant la i ème ligne et la j ème colonne. Le cofacteur i, j de A est $c_{i,j} = (-1)^{i+j} \det(A_{i,j})$.

Théorème 7.6. *Le déterminant vérifie les relations de récurrence (sur la taille n) suivante*

$i)$ Expansion selon la i ème ligne. Pour tout $1 \leqslant i \leqslant n$, et toute matrice A de $M_n(\mathbb{K})$, on a

$$\det(A) = a_{i,1}c_{i,1} + ... + a_{i,n}c_{i,n}.$$

$ii)$ Expansion selon la i ème colonne. Pour tout $1 \leqslant i \leqslant n$, et toute matrice A de $M_n(\mathbb{K})$, on a

$$\det(A) = a_{1,i}c_{1,i} + ... + a_{n,i}c_{n,i}.$$

Exemple. Calculons à l'aide de l'expansion de la deuxième ligne le déterminant $\begin{vmatrix} 2 & -1 & 2 \\ 6 & -1 & 1 \\ 4 & 5 & 3 \end{vmatrix}$.

On a

$$\begin{vmatrix} 2 & -1 & 2 \\ 6 & -1 & 1 \\ 4 & 5 & 3 \end{vmatrix} = -6 \times \begin{vmatrix} -1 & -2 \\ 5 & 3 \end{vmatrix} + (-1) \times \begin{vmatrix} 2 & -2 \\ 4 & 3 \end{vmatrix} - \begin{vmatrix} 2 & -1 \\ 4 & 5 \end{vmatrix}$$
$$= (-6) \times (-3 + 10) + (-1) \times (6 + 8) - (10 + 4) = -42 - 14 - 14 = -70$$

Si A est de taille n, cette méthode, appelée méthode des cofacteurs, nécessite de calculer $(n-2)!$ déterminant 2×2. Elle n'est efficace que jusqu'à $n = 4$ ou si on arrive à diminuer le nombre de déterminant à chaque étape (à l'aide de 0 notamment).

On va voir une autre méthode baser sur le pivot de Gauß

Définition 7.7. Soit

$$A = \begin{bmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{bmatrix}$$

une matrice carré, on appelle transposé de A et on note A^t la matrice

$$A^t = \begin{bmatrix} a_{1,1} & \dots & a_{n,1} \\ \vdots & & \vdots \\ a_{1,n} & \dots & a_{n,n} \end{bmatrix}$$

Exemple. On a $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}^t = \begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix}$.

La transposée permet en quelque sorte d'échanger les lignes et les colonnes.

Proposition 7.8. *Pour toute matrice carré A, on a* $\det(A^t) = \det(A)$.

Théorème 7.9. *Soit A une matrice de $M_n(\mathbb{K})$, on a*

$i)$ si B s'obtient de A par $L_i \leftrightarrow L_j$: $\det(B) = -\det(A)$,

$ii)$ si B s'obtient de A par $L_i \leftarrow cL_i$: $\det(B) = c\det(A)$,

$iii)$ si B s'obtient de A par $L_i \leftarrow L_i + cL_j$: $\det(B) = \det(A)$.

De même pour les opérations élémentaires sur les colonnes.

Démonstration. Comme la transposée échange lignes et colonnes et que $\det(A) = \det(A^t)$, on peut se restreindre aux opération élémentaires sur les colonnes. Notons $C_1, ..., C_n$ les colonnes de A. Montrons $i)$. Supposons que B soit obtenue de A par $C_i \leftrightarrow C_j$. On a alors

$$\begin{aligned}\det(A) &= \det(C_1, ..., C_{i-1}, C_i, C_{i+1}, ..., C_{j-1}, C_j, C_{j+1}..., C_n)\\ &= (-1)^{j-i}\det(C_1, ..., C_{i-1}, C_{i+1}, ..., C_{j-1}, C_j, C_i, C_{j+1}, ..., C_n)\\ &= (-1)^{j-i}(-1)^{j-i-1}\det(C_1, ..., C_{i-1}, C_j, C_{i+1}, ..., C_{j-1}, C_i, C_{j+1}, .., C_n)\\ &= -\det(B)\end{aligned}$$

Montrons $ii)$. Supposons que B soit obtenue de A par $C_i \leftarrow cC_i$ alors

$$\det(B) = \det(C_1, ..., cC_i, ..., C_n) = c\det(C_1, ..., C_n) = c\det(A)$$

Montrons $iii)$. Supposons que B soit obtenue de A par $C_i \leftarrow C_i + cC_j$ alors

$$\begin{aligned}\det(B) &= \det(C_1, ..., C_i + cC_j, ..., C_j, ..., C_n)\\ &= \det(C_1, ..., C_n) + c\det(C_1, ..., C_j, ..., C_j, ..., C_n)\\ &= \det(A) + 0 = \det(A) && \text{par le lemme 7.4}\end{aligned}$$

□

Lemme 7.10. *Soit A une matrice carré triangulaire supérieur (ou inférieur) alors* $\det(A) = a_{1,1}a_{2,2}...a_{n,n}$.

Exemple.

$$\begin{aligned}\begin{vmatrix}1 & 3 & 5\\ 2 & 4 & 4\\ 1 & -1 & 1\end{vmatrix} &\underset{L_2\leftarrow L_2-2L_1}{=} \begin{vmatrix}1 & 3 & 5\\ 0 & 2 & 6\\ 1 & -1 & 1\end{vmatrix} \underset{L_3\leftarrow L_3-L_1}{=} \begin{vmatrix}1 & 3 & 5\\ 0 & 2 & 6\\ 0 & -4 & -4\end{vmatrix}\\ &\underset{L_2\leftarrow -\frac{1}{2}L_2}{=} -2\begin{vmatrix}1 & 3 & 5\\ 0 & 1 & 3\\ 0 & -4 & -4\end{vmatrix} \underset{L_3\leftarrow L_3+4L_2}{=} -2\begin{vmatrix}1 & 3 & 5\\ 0 & 1 & 3\\ 0 & 0 & 8\end{vmatrix}\\ &= -2\times 8 = -16\end{aligned}$$

Au pire la méthode du pivot de Gauss nécessite $n^2 + n$ opérations de lignes c'est donc la plus efficace des que les matrices sont grandes.

3 Propriété du déterminant

Lemme 7.11. *Soit A une matrice de $M_n(\mathbb{K})$ et E une matrice ligne élémentaire. Alors* $\det(EA) = \det(E)\det(A)$.

Démonstration. A partir du théorème 7.9 et de $\det(E) = \det(E \times I_n)$, on trouve $\det(E_{i,j}) = -1$, $\det(E_i(c)) = c$ et $\det(E_{i,j}(c)) = 1$. Toujours à partir de ce même théorème, on a $\det(E_{i,j}A) = -\det(A) = \det(E_{i,j})\det(A)$ et de même pour les autres. □

Théorème 7.12. *Soit A une matrice de $M_n(\mathbb{K})$. Alors on a*

$$\det(A) \neq 0 \Leftrightarrow A \text{ est inversible}$$

Démonstration. Supposons que A se réduise par des opérations de ligne en une matrice échelonnée réduite A'. Comme le déterminant d'une matrice ligne élémentaire n'est jamais nul, on a $\det(A) = 0 \Leftrightarrow \det(A') = 0$. La matrice A' étant échelonnée, c'est une matrice triangulaire supérieur. Si A' est l'identité, et donc A est inversible, on a $\det(A') = 1$, ce qui implique $\det(A) \neq 0$. Si A' n'est pas l'identité, et donc A pas inversible, alors A' contient au moins une ligne de 0 et un élément de la diagonale de A' est nul d'où $\det(A') = \det(A) = 0$. □

Théorème 7.13. *Le déterminant est compatible avec le produit matricielle. Pour toute matrice* A, B *de* $M_n(\mathbb{K})$*, on a* $\det(AB) = \det(A)\det(B)$.

Démonstration. Premier cas : A est inversible. Il existe une suite d'opérations élémentaires réduisant A en I_n. On a donc $A = E_1 ... E_k$ où les E_i sont des matrice lignes élémentaires. On a donc

$$\begin{aligned}\det(AB) &= \det(E_1 .... E_k B) = \det(E_1) .... \det(E_k)\det(B)\\ &= \det(E_1 ... E_k)\det(B) = \det(A)\det(B)\end{aligned}$$

Deuxième cas : supposons A non inversible et donc $\operatorname{rang}(A) < n$. On a alors $\det(A) = 0$ d'où $\det(A)\det(B) = 0$. Montrons qu'on a $\det(AB) = 0$. La matrice A se réduit en une matrice échelonnée réduite A'. De ce fait $A = E_1 ... E_k A'$, où les E_i sont des matrices lignes élémentaires. On a donc

$$\det(AB) = \det(E_1 ... E_k A'B) = \det(E_1) ... \det(E_k)\det(A'B)$$

Comme on a $\operatorname{rang}(A) < n$, la matrice A' contient une ligne nulle et donc la matrice $A'B$ contient une colonne nulle, d'où $\det(AB) = 0$ □

Corollaire 7.14. *Soit* P *une matrice carré inversible alors* $\det(P^{-1}) = \frac{1}{\det(P)}$ *et* $\det(P^{-1}AP) = \det(A)$ *pour toute matrice carré* A.

Démonstration. On a $1 = \det(I_n) = \det(P^{-1}P) = \det(P^{-1})\det(P)$, d'où $\det(P^{-1}) = \frac{1}{\det(P)}$. On a $\det(P^{-1}AP) = \det(P^{-1})\det(A)\det(P) = \frac{1}{\det(P)}\det(A)\det(P) = \det(A)$. □