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. □

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 □

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 $\{1, \ldots, n\}$.

Théorème 1.15. *Pour tout entiers positifs n et k. On a équivalence entre*

$i)$ $n \leqslant k$

$ii)$ il existe une injection de $\{1, \ldots, n\}$ dans $\{1, \ldots, k\}$.

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

$$\begin{array}{rccc} f : \{1, \ldots, n\} & \to & \{1, \ldots, k\} \\ i & \mapsto & f(i) \end{array}$$

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 $\{1, \ldots, n\}$ dans $\{1, \ldots, k\}$. Pour tout entier n notons $\mathcal{P}_n$ la propriété : "s'il existe une injection de $\{1, \ldots, n\}$ dans $\{1, \ldots, n\}$, alors on a $n \leqslant k$". Montrons $\mathcal{P}_1$, pour qu'il existe une injection de $\{1\}$ dans $\{1, \ldots, k\}$ il faut et il suffit qu'il existe une application de $\{1\}$ dans $\{1, \ldots, k\}$ ce que revient à demander que l'ensemble $\{1, \ldots, k\}$ 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 $\{1, \ldots, n\}$ dans $\{1, \ldots, k\}$. Pour pouvoir utiliser l'hypothèse de récurrence $\mathcal{P}_{n-1}$ nous allons, à partir de f, construire une application de $\{1, \ldots, n-1\}$ dans $\{1, \ldots, k-1\}$. 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 $x \in \{1, \ldots, n-1\}$, 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 $f(x) \in \{1, \ldots, k-1\}$. Considérons l'application

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

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 $\{1,\dots,n\}$ 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 $\{1,\dots,n\}$.*

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

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 $\{1,\dots,n\}$ 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 $g : E \to \{1,\dots,n\}$ et $h : F \to \{1,\dots,k\}$. Supposons qu'il existe une bijection f de E sur F. Alors l'application $h \circ f$ est une bijection de E dans $\{1,\dots,k\}$ (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. □

Soit E un ensemble fini. Toute sous-ensemble de E est un ensemble fini. Pour tous sous-ensembles A et B de E, on a

– $\operatorname{Card} A \leqslant \operatorname{Card} E$

– $\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card} B - \operatorname{Card}(A \cap B)$.

Proposition 1.19. *Soient E et F des ensemble finis non vides. Si $f : E \to F$ est une application , alors on a $\operatorname{Card} f(E) \leqslant \operatorname{Card} E$. De plus, on a $\operatorname{Card} E = \operatorname{Card} F$ si et seulement si l'application f est injective.*

Démonstration. Posons $n = \operatorname{Card} E$ 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 $\operatorname{Card} f(E) = 1$ 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 $\operatorname{Card} E' = n-1$ 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

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

Par hypothèse de récurrence, on a $\operatorname{Card} g(E') \leqslant \operatorname{Card} E' = n - 1$ et donc $\operatorname{Card} f(E) \leqslant n = \operatorname{Card} E$. 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 $\operatorname{Card} g(E) = n-1$ et $f(a) \notin g(E')$, qui est encore équivalent à $\operatorname{Card} f(E) = \operatorname{Card} E$. □

Proposition 1.20 (Principe des tiroirs)**.** *Soient E, F des ensembles finis non vides et $f : E \to F$ une application. Si $\operatorname{Card} E > \operatorname{Card} F$ 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 $\operatorname{Card}(f(E)) \leqslant \operatorname{Card} F < \operatorname{Card} E$. Ainsi, par la proposition 1.19 f n'est pas injective. Il existe donc x et y dans E avec $x \neq y$ et $f(x) = f(y)$. □

Théorème 1.21. *Soient E, F des ensembles finis non vides et $f : E \to F$ une application. Si $\operatorname{Card} E = \operatorname{Card} F$, 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 $(\ ii) \operatorname{et} iii)\ ) \Rightarrow i)$. 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 $\operatorname{Card} f(E) = \operatorname{Card} F$. Or, par hypothèse, on a $\operatorname{Card} E = \operatorname{Card} F$. Ainsi f est surjective si et seulement si on a $\operatorname{Card} f(E) = E$ et donc si et seulement si f est injective d'après la proposition 1.19. □

II. Groupes

Définition 2.1. 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 2.2. *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 2.3. L'élément y introduit à la définition 2.1 et dont l'unicité est prouvé à la proposition 2.2 est appelée *inverse de* x et est notée x^{-1}.

Définition 2.4. 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 2.5. *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 2.6. 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 2.7. *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 2.8. 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 2.9. *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 2.5 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 2.5.

□

1 Groupes symétriques

Soit E un ensemble. Notons $X = E^E$ l'ensemble des applications de E dans E. Soient f et g deux éléments de X. Alors les applications $f \circ g$ et $g \circ f$ sont des éléments de E. De plus on a $f \circ \mathrm{id}_E = f$ ainsi que $\mathrm{id}_E \circ f = f$. Pour que X munis de $\circ$ soit un groupe, il ne manque plus que l'existence d'inverse pour $\circ$: pour ce faire il faut que l'application considérée soit une bijection.

Définition 2.10. Soit E un ensemble. On note $\mathfrak{S}(E)$ l'ensemble des bijections de E dans lui même.

Proposition 2.11. *L'ensemble $\mathfrak{S}(E)$ munis de la loi de composition $\circ$ est un groupe.*

Démonstration. La composée de bijection étant une bijection d'après la proposition .**??**, l'application $\circ$ est bien une loi interne de $\mathfrak{S}_n$. D'après la proposition .**??**, la loi $\circ$ est associative. L'élément neutre de $\circ$ est id_E. Si σ est un élément de $\mathfrak{S}_n$, alors par proposition .**??**, l'inverse de σ existe et est aussi une bijection par proposition .**??**. □

Définition 2.12. Le groupe *symétrique* $\mathfrak{S}_n$ est le groupe $\mathfrak{S}(\{1, \ldots, n\})$ munis de la composition $\circ$. Les éléments de $\mathfrak{S}_n$ sont appelés*permutations*.

Soit σ une permutation de $\mathfrak{S}_n$. On représente σ de la manière suivante

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$$

[Faire dessin]

Exemple. Soient $\sigma_1, \sigma_2 \in \mathfrak{S}_4$ définies par

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Alors on a [Faire dessin]

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

ainsi que

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

On remarque, en particulier, que le groupe $\mathfrak{S}_4$ n'est pas commutatif.

Définition 2.13. Un dit qu'une permutation σ de $\mathfrak{S}_n$ fixe un nombre k si $\sigma(k) = k$.

Exemple. En reprenant l'exemple précédent, σ_1 fixe 3, σ_2 ne fixe rien.

Définition 2.14. Une transposition τ de $\mathfrak{S}_n$ est une permutation qui échange deux nombres i et j et laissent fixes les autres. [Faire dessin]

Définition 2.15. Un k-cycle est une permutation σ de $\mathfrak{n}$ telle que
$\sigma(a_1) = a_2$
$\sigma^2(a_1) = \sigma(a_2) = a_3$
...
$\sigma^{k-1}(a_1) = ... = \sigma(a_{k-1}) = a_k$
$\sigma^k(a_1) = \sigma(a_k) = a_1$
et laisse fixe les autres nombres de E. On note σ par $(a_1 a_2 ... a_k)$. [Faire dessin cercle]

Remarques : Un 1-cycle est l'identité et un 2-cycle est une transposition.

Exemple.

$\tau = (24)$ de $\mathfrak{S}_4$ est la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$\sigma = (314)$ de $\mathfrak{S}_4$ est la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

chaque k-cycle admet k écritures différentes "selon l'endroit du cercle où l'on commence" :

$$\sigma = (314) = (143) = (431)$$

Définition 2.16. Le *support* d'un cycle $c = (a_1 a_2 ... a_m)$, noté $\mathrm{supp}(c)$, est le sous-ensemble $\{1, ..., m\}$ de E. On dit que deux cycles c_1 et c_2 sont à *support s disjoints* si $\mathrm{supp}\, c_1 \cap \mathrm{supp}\, c_2$ est vide.

Lemme 2.17. *Soient c_1 et c_2 deux cycles de $\mathfrak{S}_n$ à supports disjoints alors c_1 et c_2 commutent, c'est-à-dire, $c_1 c_2 = c_2 c_1$.*

Démonstration. Pour $k \in \mathrm{supp}(c_1)$, on a $c_1 \circ c_2(k) = c_1(k)$ et $c_2 \circ c_1(k) = c_1(k)$. Pour $k \in \mathrm{supp}(c_2)$, on a $c_1 \circ c_2(k) = c_2(k)$ et $c_2 \circ c_1(k) = c_2(k)$. Pour $k \in \{1, ..., n\} \setminus (\mathrm{supp}(c_1) \cup \mathrm{supp}(c_2)$, on a $c_1 \circ c_2(k) = c_1(k) = k$ et $c_2 \circ c_1(k) = c_2(k) = k$. Dans les trois cas, on obtient $c_1 \circ c_2(k) = c_2 \circ c_1(k)$ et donc les cycles c_1 et c_2 commutent. □

Exemple. Les cycles $c_1 = (14)$ et $c_2 = (23)$ de $\mathfrak{S}_4$ commutent.

Définition 2.18. Soit σ une permutation de $\mathfrak{S}_n$. Une *orbite* de σ est une liste $< a_1, a_2, ..., a_r >$ de $\{1, ..., n\}$ telle que
$a_2 = \sigma(a_1)$
$a_3 = \sigma(a_2) = \sigma^2(a_1)$
...
$a_r = \sigma(a_{r-1}) = ... = \sigma^{r-1}(a_1)$
$a_1 = \sigma(a_r)$

Exemple. Les orbites de la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

sont $< 1, 2, 4 >$ et $< 3 >$.

Théorème 2.19. *Une permutation σ de $\mathfrak{S}_n$ est le produit des cycles correspondant à ses orbites. C'est l'unique écriture (à ordre près) de σ comme produit de cycle à support disjoints.*

Démonstration. On utilise une récurrence sur l'entier n, l'affirmation étant claire pour $n = 3$ (puisque toutes les permutations sont alors des cycles). Supposons donc l'énoncé démontré pour les permutations de $\mathfrak{S}_k$ éléments avec $k < n$ et considérons $\sigma \in \mathfrak{S}_n$. En regardant la suite 1, $\mathfrak{S}_1$, ... on remarque qu'il existe un plus petit entier $m \geqslant 1$ tel que $\sigma^m(1) = 1$ (on n'exclut pas $m = 1$). Définissons l'ensemble $I = \{1, \sigma(1), \sigma^2(1), ..., \sigma^{m-1}(1)\}$ et le m-cycle $c = (1, \sigma(1)\sigma^2(1)..., \sigma^{m-1}(1))$; alors la permutation $\tau = \sigma c^{-1}$laisse fixe les éléments de I et pour $i \notin I$ on a $\tau(i) = \sigma(i)$. La restriction de τ a $J = \{1, ..., n\} \setminus I$ est donc une permutation des éléments de J que nous notons σ'. Comme $\#J < n$, on sait (par l'hypothèse de récurrence) que $\sigma' = c'_1 \cdot ... \cdot c'_k$ avec c'_i des cycles de J à supports disjoints. On construit des cycles i de $\mathfrak{S}_n$, en posant

$$c_i(j) = \begin{cases} c'_i(j) & \text{pour } i \in J \\ j & \text{sinon} \end{cases}$$

On a alors $\tau = c_1 \cdot ... \cdot c_k$ et donc $\sigma = c_1 \cdot ... \cdot c_k \cdot c$. Ceci prouve l'existence de la décomposition en cycles ; pour l'unicité on observe que le cycle c est uniquement déterminé par σ et que par hypothèse de récurrence les cycles $c'_1, ..., c'_k$ sont uniques. □

Exemple. Considérons la permutation σ de $\mathfrak{S}_n$ définie par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 1 & 6 & 7 & 3 & 5 & 4 & 8 & 2 \end{pmatrix}$$

Les orbites de σ sont $< 1, 9, 2 >, < 3, 6, 5 >, < 4, 7 >$ et $< 8 >$ On a donc $\sigma = (192)(365)(47)(8) = (192)(365)(47)$.

Définition 2.20. On dit qu'un groupe G est engendré par $\{g_1, g_2, ..., g_r\}$ si chaque élément de G est un produit de g_i et g_i^{-1}.

Une conséquence immédiate du théorème précédent est

Corollaire 2.21. *$\mathfrak{S}_n$ est engendré par ses cycles.*

Proposition 2.22. *$\mathfrak{S}_n$ est engendré par ses transpositions*

Démonstration. Il suffit de montrer que chaque cycle peut être écris comme produit de transpositions. On a $(12)^2 = e$ donc l'identité est bien produit de transposition. Démontrons par récurrence sur k qu'un k-cycles est produit de transpositions. Puisque qu'un 2-cycle est une transposition, la propriété est vraie pour $k = 2$. Supposons l'entier k supérieur ou égale à 3 et la propriété vraie pour l'entier $k - 1$. Soit $\sigma = (a_1 a_2 ... a_k)$ un k-cycle. Nous avons $s = (a_1 a_2)(a_2 a_3 ... a_k)$. Par hypothèse de récurrence le $(k-1)$-cycle $(a_2 a_3 ... a_k)$ est produit de transpositions, par suite σ l'est aussi. □

Exemple. Considérons la permutation σ de $\mathfrak{S}_n$ définie par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 1 & 6 & 7 & 3 & 5 & 4 & 8 & 2 \end{pmatrix}$$

On a déjà vu $\sigma = (192)(365)(47)(8) = (192)(365)(47)$. On a $(192) = (19)(92)$ et $(365) = (36)(65)$ et donc

$$\sigma = (19)(92)(36)(65)(47).$$

Attention, la décomposition d'une permutation comme produit de transposition n'est pas unique : On vérifie $(143) = (14)(43)$ et $(143) = (12)(23)(24)(12)$.

Définition 2.23. Soit σ une permutation de $\mathfrak{S}_n$. La *signature* de σ, notée $\varepsilon(\sigma)$ est

$$\varepsilon(\sigma) = \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(i)-\sigma(j)}{i-j}$$

où $\mathcal{P}$ est l'ensemble des paires $\{i,j\}$ avec $i \neq j$.

Exemple. Soit σ la permutation de $\mathfrak{S}_4$ définie par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

On a $\mathcal{P} = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$ et donc

$$\begin{aligned}
\varepsilon(\sigma) &= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(i)-\sigma(j)}{i-j} \\
&= \frac{\sigma(1)-\sigma(2)}{1-2}\,\frac{\sigma(1)-\sigma(3)}{1-3}\,\frac{\sigma(1)-\sigma(4)}{1-4}\,\frac{\sigma(2)-\sigma(3)}{2-3}\,\frac{\sigma(2)-\sigma(4)}{2-4}\,\frac{\sigma(3)-\sigma(4)}{3-4} \\
&= \frac{2-4}{1-2}\,\frac{2-3}{1-3}\,\frac{2-1}{1-4}\,\frac{4-3}{2-3}\,\frac{4-1}{2-4}\,\frac{3-1}{3-4} \\
&= \frac{-2}{-1}\,\frac{-1}{-2}\,\frac{1}{-3}\,\frac{1}{-1}\,\frac{3}{-2}\,\frac{-2}{-1} = \frac{-12}{12} = -1
\end{aligned}$$

Lemme 2.24. *Soient σ et τ deux permutations de $\mathfrak{S}_n$, alors on a $\varepsilon(\sigma\circ\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.*

Démonstration.

$$\begin{aligned}
\varepsilon(\sigma\circ\tau) &= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma\circ\tau(i)-\sigma\circ\tau(j)}{i-j} = \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{i-j} \\
&= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)}\,\frac{\tau(i)-\tau(j)}{i-j} \\
&= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} \prod_{\{i,j\}\in\mathcal{P}} \frac{\tau(i)-\tau(j)}{i-j} \\
&= \prod_{\{\tau(i),\tau(j)\}\in\mathcal{P}} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} \prod_{\{i,j\}\in\mathcal{P}} \frac{\tau(i)-\tau(j)}{i-j} \\
&= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(i)-\sigma(j)}{i-j} \prod_{\{i,j\}\in\mathcal{P}} \frac{\tau(i)-\tau(j)}{i-j} \\
&= \varepsilon(\sigma)\varepsilon(\tau)
\end{aligned}$$

□

Lemme 2.25. *Soit σ une transposition de $\mathfrak{S}_n$, alors on a $\varepsilon(\sigma) = -1$.*

Démonstration. Posons $\sigma = (k\,\ell)$ avec $k < \ell$ ainsi que

– $\mathcal{Q} = \{\{i,j\}\text{avec } i,j \neq k\}$,
– $\mathcal{P}_1 = \{\{i,k\}\text{avec } i < k\}$,
– $\mathcal{P}_2 = \{\{k,j\}\text{avec } k < j < \ell\}$,
– $\mathcal{P}_3 = \{\{k,j\}\text{avec } \ell < j\}$,
– $\mathcal{P}_4 = \{\{i,\ell\}\text{avec } i < k\}$,
– $\mathcal{P}_5 = \{\{i,\ell\}\text{avec } k < i < \ell\}$,
– $\mathcal{P}_6 = \{\{\ell,j\}\text{avec } \ell < j\}$,
– $\mathcal{R} = \{\{k,\ell\}\}$.

On a alors $\mathcal{P} = \mathcal{Q} \sqcup \mathcal{P}_1 \sqcup \mathcal{P}_2 \sqcup \mathcal{P}_3 \sqcup \mathcal{P}_4 \sqcup \mathcal{P}_5 \sqcup \mathcal{P}_6 \sqcup \mathcal{R}$ et donc

$$\begin{aligned}\varepsilon(\sigma) &= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(i)-\sigma(j)}{i-j} \\ &= \prod_{\{i,j\}\in\mathcal{Q}} \frac{\sigma(i)-\sigma(j)}{i-j} \prod_{\{i,j\}\in\mathcal{P}_1} \frac{\sigma(i)-\sigma(j)}{i-j} \prod_{\{i,j\}\in\mathcal{P}_2} \frac{\sigma(i)-\sigma(j)}{i-j} \prod_{\{i,j\}\in\mathcal{P}_3} \frac{\sigma(i)-\sigma(j)}{i-j} \\ &\quad \prod_{\{i,j\}\in\mathcal{P}_4} \frac{\sigma(i)-\sigma(j)}{i-j} \prod_{\{i,j\}\in\mathcal{P}-5} \frac{\sigma(i)-\sigma(j)}{i-j} \prod_{\{i,j\}\in\mathcal{P}_6} \frac{\sigma(i)-\sigma(j)}{i-j} \prod_{\{i,j\}\in\mathcal{R}} \frac{\sigma(i)-\sigma(j)}{i-j}\end{aligned}$$

On calcule

$$\begin{aligned}\prod_{\{i,j\}\in\mathcal{Q}} \frac{\sigma(i)-\sigma(j)}{i-j} &= \prod_{\{i,j\}\in\mathcal{Q}} \frac{i-j}{i-j} = 1 \\ \prod_{\{i,j\}\in\mathcal{P}_1} \frac{\sigma(i)-\sigma(j)}{i-j} &= \prod_{i<k} \frac{\sigma(i)-\sigma(k)}{i-k} = \prod_{i<k} \frac{i-\ell}{i-k} \\ \prod_{\{i,j\}\in\mathcal{P}_2} \frac{\sigma(i)-\sigma(j)}{i-j} &= \prod_{k<j<\ell} \frac{\sigma(k)-\sigma(j)}{k-j} = \prod_{k<j<\ell} \frac{\ell-j}{k-j} \\ \prod_{\{i,j\}\in\mathcal{P}_3} \frac{\sigma(i)-\sigma(j)}{i-j} &= \prod_{\ell<j} \frac{\sigma(k)-\sigma(j)}{k-j} = \prod_{\ell<j} \frac{\ell-j}{k-j} \\ \prod_{\{i,j\}\in\mathcal{P}_4} \frac{\sigma(i)-\sigma(j)}{i-j} &= \prod_{i<k} \frac{\sigma(i)-\sigma(\ell)}{i-\ell} = \prod_{i<k} \frac{i-k}{i-\ell} \\ \prod_{\{i,j\}\in\mathcal{P}_5} \frac{\sigma(i)-\sigma(j)}{i-j} &= \prod_{k<i<\ell} \frac{\sigma(i)-\sigma(\ell)}{i-\ell} = \prod_{k<i<\ell} \frac{i-k}{i-\ell} \\ \prod_{\{i,j\}\in\mathcal{P}_6} \frac{\sigma(i)-\sigma(j)}{i-j} &= \prod_{\ell<j} \frac{\sigma(\ell)-\sigma(j)}{\ell-j} = \prod_{\ell<j} \frac{k-j}{\ell-j} \\ \prod_{\{i,j\}\in\mathcal{R}} \frac{\sigma(i)-\sigma(j)}{i-j} &= \frac{\sigma(k)-\sigma(\ell)}{k-\ell} = \frac{\ell-k}{k-\ell} = -1\end{aligned}$$

On a donc

$$\begin{aligned}\varepsilon(\sigma) &= 1 \cdot \prod_{i<k} \frac{i-\ell}{i-k} \cdot \prod_{k<j<\ell} \frac{\ell-j}{k-j} \cdot \prod_{\ell<j} \frac{\ell-j}{k-j} \cdot \prod_{i<k} \frac{i-k}{i-\ell} \cdot \prod_{k<i<\ell} \frac{i-k}{i-\ell} \cdot \prod_{\ell<j} \frac{k-j}{\ell-j} \cdot -1 \\ &= -\prod_{i<k} \frac{i-\ell}{i-k} \cdot \prod_{i<k} \frac{i-k}{i-\ell} \cdot \prod_{\ell<j} \frac{\ell-j}{k-j} \cdot \prod_{\ell<j} \frac{k-j}{\ell-j} \cdot \prod_{k<j<\ell} \frac{\ell-j}{k-j} \cdot \prod_{k<i<\ell} \frac{i-k}{i-\ell} \\ &= -\prod_{k<j<\ell} \frac{\ell-j}{k-j} \cdot \prod_{k<i<\ell} \frac{i-k}{i-\ell} \\ &= -\prod_{k<i<\ell} \frac{\ell-i}{k-i} \cdot \prod_{k<i<\ell} \frac{i-k}{i-\ell} \\ &= -1\end{aligned}$$

□

Proposition 2.26. *Pour tout n, la signature ε est un morphisme de $(\mathfrak{S}_n, \circ)$ sur $(\{-1,1\}, \times)$.*

Démonstration. Soit σ une permutation de $\mathfrak{S}_n$. Par la proposition 2.22, σ est produit de transposition, disons $\sigma = \tau_1 \cdot ... \cdot \tau_k$. Le lemme 2.24 implique donc $\varepsilon(\sigma) = \varepsilon(\tau_1) \cdot ... \cdot \varepsilon(\tau_k)$, ce qui en utilisant le lemme 2.25 donne $\varepsilon(\sigma) = (-1)^k$. La signature est donc une application de $\mathfrak{S}_n$ dans l'ensemble $\{-1,1\}$ qui se trouve être un morphisme par le lemme 2.24. □

Corollaire 2.27. *Soit σ une permutation de $\mathfrak{S}_n$. La décomposition $\sigma = \tau_1 \cdot ... \cdot \tau_k$ n'est pas unique mais le nombre de transpositions nécessaires est de la même parité que k et on a $\varepsilon(\sigma) = (-1)^k$.*

Démonstration. Soit $\sigma = \tau'_1 \cdot ... \cdot \tau'_\ell$ ne autre décomposition. Alors on a

$$(-1)^\ell = \varepsilon(\tau'_1 \cdot ... \cdot \tau'_\ell)\varepsilon(\sigma) = (-1)^k$$

Les entiers k et ℓ sont donc tous les deux pairs ou tous les deux impairs. □

Proposition 2.28. *La signature d'un k-cycle est $(-1)^{k-1}$*

Démonstration. Soit $c = (a_1 ... a_k)$ un k-cycle. On a donc $c = (a_1 a_2)(a_2 a_3)...(a_{k-1} a_k)$ puis $\varepsilon(c) = (-1)^{k-1}$. □

Corollaire 2.29. *Si $\sigma \in \mathfrak{S}_n$ se décompose en ℓ cycles à support disjoint (en tenant compte aussi de cycle de longueur 1), on a $\varepsilon(\sigma) = (-1)^{n-\ell}$.*

Démonstration. Soit $\sigma = c_1 \cdot ... \cdot c_\ell$ la décomposition de σ en cycle à support disjoint. Notons k_i la longueur de c_i. On a alors

$$\varepsilon(\sigma) = \prod_{i=1}^{\ell} (-1)^{k_i - 1} = (-1)^{-\ell} \prod_{i=1}^{\ell} (-1)^{k_i} = (-1)^{-\ell} \cdot (-1)^{\sum_{i=1}^{\ell} k_i} = (-1)^\ell \cdot (-1)^n = (-1)^{n-\ell}$$

□

Pour calculer la signature d'une permutation il suffit donc de la décomposer en cycle à support disjoint.

Exemple. Reconsidérons la permutation σ de $\mathfrak{S}_9$ définie par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 1 & 6 & 7 & 3 & 5 & 4 & 8 & 2 \end{pmatrix}$$

On a déjà vu $\sigma = (192)(365)(47)(8)$. On a donc $\varepsilon(\sigma) = (-1)^{9-4} = (-1)^5 = -1$

2 Relations d'équivalences

Définition 2.30. Une *relation* $\mathcal{R}$ sur un ensemble E est un sous-ensemble $\mathcal{R} \subseteq E \times E$. On note l'appartenance $(x, y) \in \mathcal{R}$ par $x\mathcal{R}y$.

Définition 2.31. On dit qu'une relation $\mathcal{R}$ sur un ensemble E est une relation d'*équivalence* si elle est

– *réflexive* : pour tout $x \in E$, on a $x\mathcal{R}x$;
– *symétrique* : pour tous $x, y \in E$, on a $x\mathcal{R}y \Rightarrow y\mathcal{R}x$;
– *transitive* : pour tous $x, y, z \in E$, on a $x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$.

Exemple. Soit $n \in \mathbb{N}$. Pour tout $a, b \in \mathbb{N}$, on pose $a \equiv b \mod n$ si n divise $b - a$. C'est la *congruence modulo* n. La relation $\equiv$ est une relation d'équivalence sur $\mathbb{N}$. [Faire démo au tableau]

Définition 2.32. Soit $\mathcal{R}$ une relation d'équivalence sur E. Une *classe d'équivalence* est un sou-ensemble

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

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 2.33. 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 2.34. *Soit $\mathcal{R}$ une relation d'équivalence sur E. Alors les classes d'équivalences de $\mathcal{R}$ 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'équiva lence

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

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 $\mathcal{E}_\mathcal{R} = \{0, 1, 2, 3, 4\}$.

3 Classes à gauche

Proposition 2.35. *Soit G un groupe, H un sous-groupe de G. Alors la relation $\mathcal{R}_H$ sur G définie par*

$$x \mathcal{R}_H y \Leftrightarrow x^{-1}y \in H$$

est une relation d'équivalence.

Vérification directe au tableau. □

Définition 2.36. Soit G un groupe et H un sous-groupe de G. La classe à gauche d'un élément $x \in G$ est l'ensemble, noté $x \cdot H$, défini par

$$x \cdot H = \{x \cdot h \mid h \in H\}$$

Proposition 2.37. *Soit G un groupe et H un sous-groupe de G. Les classes à gauches, sont les classes d'équivalences de $\mathcal{R}_H$. Plus précisèment, pour tout $x \in G$ on a $[x]_{\mathcal{R}_H} = x \cdot H$.*

Démonstration. Montrons $[x]_{\mathcal{R}_H} \subseteq x \cdot H$. Soit $y \in [x]_{\mathcal{R}_H}$. On a $y \mathcal{R}_H x$, à savoir que $x^{-1}y \in H$. Il existe donc $h \in H$ tel que $x^{-1}y = h$, d'où $y = x \cdot H$, et donc $y \in x \cdot H$.

Montrons $x \cdot H \subseteq [x]_{\mathcal{R}_H}$. Soit $y \in x \cdot H$. Il existe $h \in H$ tel que $y = x \cdot h$. On a donc $x^{-1}y = h$ puis $x^{-1}y \in H$.

□

Exemple. On a $\mathfrak{S}_3 = \{e, (12), (13), (23), (123), (132)\}$. Soit H_1 le sous-groupe de $\mathfrak{S}_3$ définie par $H_1 = \{e, (12)\}$. Les classes à gauches sont

$$\begin{aligned}
e \cdot H_1 &= \{e, (12)\} \\
(13) \cdot H_1 &= \{(13), (123)\} \\
(23) \cdot H_1 &= \{(23), (132)\}.
\end{aligned}$$

Soit H_2 le sous-groupe de $\mathfrak{S}_3$ définie par $H_2 = \{e, (123), (132)\}$. Les classes à gauches sont :

$$\begin{aligned}
e \cdot H_2 &= \{e, (123), (132)\} \\
(12) \cdot H_1 &= \{(12), (23), (13)\}
\end{aligned}$$

Lemme 2.38. *Soient G un groupe, H un sous-groupe de G et $x\cdot H, y\cdot H$ deux classes à gauches. Alors l'application*

$$\begin{aligned}\psi :& x\cdot H \to y\cdot H\\ & x\cdot h \mapsto y\cdot h\end{aligned}$$

est une bijection.

Démonstration. Injectivité : $\psi(x\cdot h_1)=\psi(x\cdot h_2)$ implique $y\cdot h_1 = y\cdot h_2$ et donc $h_1=h_2$. Surjectivité : Soit $z\in y\cdot H$. Il existe alors $h\in H$ tel que $z=y\cdot h$. On a alors $\psi(x\cdot h)=z$. □

Corollaire 2.39. *Soit G un groupe et H uns sous-groupe de G. Si H est fini (= nombre fini d'éléments), toutes les classes à gauche ont sont de cardinalité* $\mathrm{Card}(H)$.

Démonstration. Comme $H=e\cdot H$, H est une classe à gauche. Par le lemme précédant, toutes les classes gauches étant en bijection, elles sont donc fini et ont même cardinal que H. □

Définition 2.40. Soit G un groupe fini. L'*ordre* de G est la cardinalité de G, on le note $o(G)$.

Théorème 2.41 (de Lagrange)**.** *Soient G un groupe fini et H un sous-groupe de G. Alors $o(H)$ divise $o(G)$.*

Démonstration. G se partitionne en les classes d'équivalence de $\mathcal{R}_H$, à savoir en classe à gauche. Comme G est fini, il y a un nombre fini m de classes :

$$G=\bigsqcup_{i=1}^{n} c_i\cdot H$$

On a alors

$$o(G)=\mathrm{Card}(G)=\sum_{i=1}^{m}\mathrm{Card}(x_i\cdot H)=m\,\mathrm{Card}(H)=mo(H)$$

□

Exemple. $o(\mathfrak{S}_3)=6$. Par le théorème de Lagrange, $\mathfrak{S}_3$ ne peut pas avoir un sous groupe à 4 éléments.

Définition 2.42. On dit qu'un groupe G est *cyclique* (monogène) s'il est est engendré par un seul élément. Si $g\in G$ est un tel élément, on note $G=<g>$.

Proposition 2.43. *Deux groupes cycliques ayant m éléments sont isomorphes (sont le même groupe au noms des éléments près).*

Démonstration. Soient G et H deux groupes cycliques ayant m éléments. Posons $G=<g>$ et $H=<h>$. Notons $\psi : G\to H$ définie par $\psi(g)=h$. L'application ψ est un morphisme de groupe :

$$\psi(g^i\cdot g^j)=\psi(g^{i+j})=h^{i+j}=h^i\cdot h^j=\psi(g^i)\cdot\psi(h^j).$$

Comme G et H sont fini et ont même nombre d'élément, ψ est bijective si elle est surjective, par Théorème I.1.21. Tout élément de H est de la forme h^i. Ainsi, la relation $\psi(g^i)=h^i$ montre que ψ est surjective. L'application ψ est donc un isomorphisme. Il s'en suit que G et H sont isomorphes. □

Définition 2.44. Soit G un groupe. L'*ordre* de $x \in G$ et le plus petit $n \geqslant 1$, s'il existe, tel que $x^n = e$. On le note $o(a)$. Si un tel n n'existe pas, on dit que a est d'ordre infini.

Si G est un groupe fini, tous ses éléments sont d'ordres fini. Pour $x \in G$, la suite $x, x^2, x^3, ...$ doit avoir des répétitions. Il existe donc $i \neq j$ avec $x^i = x^j$ et donc $x^{i-j} = e$. L'ensemble $\{k \geqslant 1 \mid x^k = e\}$ n'étant pas vide, il admet un plus petit élément, à savoir $o(x)$.

Lemme 2.45. *Soit G un groupe finie. Pour tout $x \in G$, l'ordre de x est l'ordre du groupe cyclique engendré par x.*

Démonstration. Posons $E_+ = \{e, x, x^2, ...\}$et $E_- = \{x^{-1}, x^{-2}, ...\}$. On a $< x >= E_+ \cup E_-$. Posons $n = o(x)$. On a $x^n = e$, d'où $x^{n-1} = x^{-1}$. On en déduit $x^{-1}E^+$ puis $E_- \subseteq E_+$. Soit $k \geqslant 1$. Par le théorème de la division euclidienne $k = qn + r$ avec $r \in \{0, ..., n-1\}$. On a donc $x^k = x^{qn+r} = x^r$. D'où $E_+ = \{e, x, ..., x^{n-1}\}$ et donc $< x >= \{e, x, ..., x^{n-1}\}$. Pour le moment nous avons seulement $o(< x >) \leqslant o(x)$. Supposons par l'absurde $o(< x >) < o(x)$. Dans ce cas, deux éléments de la liste $e, x^2, ..., x^{n-1}$ doivent être égaux. Disons x^i et x^j avec $i < j$. On a alors $e = x^{j-i}$. Or $j - i$ est plus petit que n, ce qui est en contradiction avec la définition de $o(x) = n$. □

Proposition 2.46. *Soit G un groupe finie. Pour tout $x \in G$, $o(x)$ divise $o(G)$.*

Démonstration. $< x >$ est sous-groupe de G. Donc, par le théorème de Lagrange, $o(< x >)$ est un diviseur de $o(G)$. Comme $o(x) = o(< x >)$, l'ordre de x divise l'ordre de G. □

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

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

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. □

IV. Les anneaux

1 Définition de base

Définition 4.1. 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 4.2. 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 4.3. 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 4.4. 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 4.5. *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. □

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

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

2 Arithmérique

Fait : L'ensemble $\mathbb{Z}$ munis de l'addition et de la multiplication usuelle est un anneau commutatif.

Définition 4.7. Soeint a et b deux éléments de $\mathbb{Z}$. On dit que a *divise* b ou que b est un *multiple* de a s'il existe $c \in \mathbb{Z}$ tel que $b = ac$.

Définition 4.8. Un nombre p de $\mathbb{Z}$ est dit *premier* s'il possède exactement deux diviseurs : 1 et n.

Exemple. Les nombre $2, 3, 5, -5, 11$ sont premiers tandis que $4, 6, -8, 1, -1$ ne le sont pas.

La propriété la plus importante de l'anneau $\mathbb{Z}$ est l'existence de la *division euclidienne*.

Théorème 4.9. *Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$ alors il existe des uniques $q, r \in \mathbb{Z}$ avec $0 \leqslant r \leqslant \mid b \mid$ avec $a = bq + r$.*

Démonstration. Suppososns d'abors pour simplifier que b soit positif. On regarde le suite des multiples (positifs ou négatifs) de b. Soit q le plus grand entier tel que $qb \leqslant a$. On alors $qb \leqslant a < (q+1)b$. Posons $r = a - bq$. Il vient alors $0 \leqslant r < b$ d'où le résultat. Si b est négatif, on procède de même qvec $-a$ et $-b$: on obtient $-a = q'(-b) + r'$ aevc $0 \leqslant r_1 < -b$ d'où $a = q'b - r'$ Si r' est nul c'est bon. Sinon on écrit $a = (q'+1)b + (-b - r')$ et on pose $q = q' + 1$ et $r = -b + r'$. On a alors $0 \leqslant r = (-b - r') < -b = \mid b \mid$.

Pour prouver l'unicité, on suppose que $a = bq + r = bq' + r'$ avec $0 \leqslant r, r' < \mid b \mid$. On obtient alors $\mid b \mid\mid q - q' \mid = \mid r - r' \mid < \mid b \mid$, ce qui entraîne $\mid q - q' \mid = 0$ et qonc $q = q'$ puis $r = r'$. □

Théorème 4.10. *Les sous-groupes de $\mathbb{Z}$ sont tous de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.*

Démonstration. Soit G un sous groupe de Z. Si $G = \{0\}$, on a $G = 0\mathbb{Z}$. Sinon, il existe un plus petit n strictement positif dans G. L'ensemble des multiples de n devant être inclut dans G, on a $n\mathbb{Z} \subseteq G$. Soit g un élément de G. La division eculidienne de g par n donne $g = nq + r$ avec $0 \leqslant r < n$. L'entier $r = g - nq$ est un élément de G. Ce qui par construction de n implique $r = 0$. Il s'en suit que g est un multiple de n. On a donc $G = n\mathbb{Z}$. □

Définition 4.11. Soient a et b des éléments de $\mathbb{Z}$. Le plus grand diviseur commun de a et b, noté $\mathrm{pgcd}(a, b)$ est un entier d vérifiant

$i)$ d divise a et d divise b

$ii)$ si d' divise a et d' divise b alors d' divise d.

Exemple. $\mathrm{pgcd}(12, 15) = 3$, $\mathrm{pgcd}(25, 9) = 1$, $\mathrm{pgcd}(16, 6) = 2$.

Définition 4.12. Soient $a, b \in \mathbb{Z}$, on pose

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

Proposition 4.13. *Soient $a, b \in \mathbb{Z} - \{0\}$. On a $a\mathbb{Z} + b\mathbb{Z} = \mathrm{pgcd}(a, b)\mathbb{Z}$.*

Démonstration. Soient x et x' des éléments de $a\mathbb{Z} + b\mathbb{Z}$. Il existe alors u,v,u' et v' vérifiat $x = au + bv$, $x' = au' + bv'$. On a alors $x + x' = a(u + u') + b(v + v')$ et $-x = a(-u) + b(-v)$. On en deduit $x + x' \in a\mathbb{Z} + b\mathbb{Z}$ et $-x \in a\mathbb{Z} + b\mathbb{Z}$. L'ensemble $a\mathbb{Z} + b\mathbb{Z}$ est donc un sous-groupe de $\mathbb{Z}$. Il existe donc $d \in \mathbb{Z}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Montrons $d = \mathrm{pgcd}(a, b)$. De $a = a \cdot 1 + b \cdot 0$ et $b = a \cdot 0 + 1 \cdot 1$, on déduit que d est un diviseur de a et b. On peut aussi écrire $d = au + bv$ pour certains entiers u et v. Par conséquent tout diviseur commun à a et b est un diviseur de d. On a donc $d = \mathrm{pgcd}(a, b)$. □

Définition 4.14. Deux entiers $a, b \in \mathbb{Z}$ sont dits premiers entre eux si $\text{pgcd}(a, b) = 1$.

Théorème 4.15 (Bezout)**.** *Soient $a, b \in \mathbb{Z}$, alors il existe deux entiers u et v tels que $au+bv = q$. En particulier, deux entiers a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tels que $au + vb = 1$.*

Démonstration. La première partie du théorème est une conséquence directe de la proposition précédente. Pour la deuxième partie, notons que si $\text{pgcd}(a, b) = 1$ alors il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$; inversemeent si de tels u, v existent, alors un divideur d de a et b diviserait $au + bv$ et donc 1 ce qui donne bien que a eet b sont premiers entre eux. □

Exemple. $15 - 12 = 3 = \text{pgcd}(12, 15)$, $4 \times 25 - 11 \times 9 = 1$, $-1 \times 16 + 3 * 6 = 2$.

Théorème 4.16 (Euclide)**.** *Soit p un nombre premier, si p divise ab alors p divise a ou p divise b.*

Démonstration. Si p ne divise pas a alors $1 = \text{pgcd}(a, p) = pu + av$, se qui implique $b = pbu + abv$ puis p divise b. □

Théorème 4.17 (Gauss)**.** *Si $a, b \in \mathbb{Z}$ sont premiers entre eux et a divise bc alors a divise c*

Démonstration. On a $1 = \text{pgcd}(a, b) = au + bv$ donc $c = cau + cbv$ puis a divise c. □

Théorème 4.18. *Il existe une infinité de nombre premier.*

3 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Rappel : soient $a, b, n \in \mathbb{Z}$, on a $a \equiv b \mod n$ si n divise $b - a$.

Lemme 4.19. *Soient a, b, c, d des éléments de $\mathbb{Z}$ vérifiant $a \equiv b \mod n$ et $c \equiv d \mod n$. Alors on a $a + c \equiv b + d \mod n$ et $a \cdot c \equiv b \cdot d \mod n$.*

Démonstration. Comme $a \equiv b \mod n$ et $c \equiv d \mod n$, il existe k et k' vérifiant $a = b + kn$ et $c = d + k'n$. On a alors $a + c = b + kn + d + k'n = (c + d) + (k + k')n$ et $a \cdot c = (b + kn) \cdot (c + k'n) = bc + bk'n + knc + knk'n = bc + (bk' + kc + kk'n)n$. 'entier n divise donc $(a + c) - (b + d)$ et $ac - bd$. On a donc $a + c \equiv b + d \mod n$ et $ac \equiv bd \mod n$. □

Définition 4.20. Soit $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences de la congruence modulo n. Muni des opérations $+$ et $\cdot$ définies par

$$[x] + [y] = [x + y] \quad \text{et} \quad [x] \cdot [y] = [x \cdot y]$$

c'est un anneau commutatif

Remarque : Pour pouvoir définir les opérations sur les classes d'équivalence, la définition de ces opérations ne doit pas dépendre du choix des représentants des classes d'équivalences. 'Cest le cas pour $\mathbb{Z}/n\mathbb{Z}$. Si$[x_1] = [x_2]$ (x_1, x_2 représentant de la même classe) et $[y_1] = [y_2]$ alors on a $x_1 \equiv x_2 \mod n$ et $y_1 \equiv y_2 \mod n$. On conclut alors à l'aide du lemme précédant.

Par convention, on note $\overline{x}$ la classe de x et on considérera $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.

Exemple. $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{1}, \overline{3}\}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Observation : on a $\overline{2} \cdot \overline{2} = 0$. Les éléments inversibles sont $\overline{1}$ et $\overline{3}$.

Proposition 4.21. *Le groupe multiplicatif de $\mathbb{Z}/n\mathbb{Z}$ est*

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{x} \mid \operatorname{pgcd}(x, n) = 1\}.$$

Démonstration. Posons $E = \{\overline{x} \mid \operatorname{pgcd}(x, n) = 1\}$. Montrons $E \subseteq (\mathbb{Z}/n\mathbb{Z})^*$. Soit $\overline{x}$ un élment de E Comme $\operatorname{pgcd}(x, n)$ vaut 1, le théorème de Bezout assure l'existence de u et v dans $\mathbb{Z}$ vérifiant $ux + vn = 1$. On a donc $ux \equiv 1 \mod n$ puis $\overline{ux} = 1$ et enfin $\overline{u} \cdot \overline{x} = 1$. L'élement $\overline{x}$ admet donc $\overline{u}$ comme inverse.

Montrons $(\mathbb{Z}/n\mathbb{Z})^* \subseteq E$. Si x est un élément de $(\mathbb{Z}/n\mathbb{Z})^*$, il existe $\overline{y}$ tel que $\overline{y} \cdot \overline{x} = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$. On a donc $ax = 1 \mod n$ et l'existence de $b \in \mathbb{Z}$ vérifiant $ax + bn = 1$. Ce qui implique $\operatorname{pgcd}(x, n) = 1$. □

Définition 4.22. Soit $n \geqslant 2$. La fonction ϕ d'Euler est définie ar $\phi(n) = \operatorname{Card}((\mathbb{Z}/n\mathbb{Z})^*)$. $\phi(n)$ est le nombre d'entier compris entre 1 et $n - 1$ premier avec n.

Exemple. Pour $n = 12$, on a $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ et $\phi(n) = 4$. Pour $n = 15$, on a $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$ et $\phi(n) = 8$

Lemme 4.23. *Si a et premier avec n, on a $a^{\phi(n)} \equiv 1 \mod n$.*

Démonstration. Une des conséquences du théorème de Lagrange est que l'ordre de l'élément $a \in (\mathbb{Z}/n\mathbb{Z})^*$ soit un diviseur de $o((\mathbb{Z}/n\mathbb{Z})^*) = \phi(n)$. Il existe donc un entier k vérifiant $\phi(n) = ko(a)$. On obtient alors

$$a^{\phi(n)} = (a^{o(a)})^k = 1^k = 1,$$

et donc $a^{\phi(n)} \equiv 1 \mod n$. □

Théorème 4.24. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corms si et seulement si n est premier*

Démonstration. Si n n'est pas premier, alors $n = ab$ avec $a, b \neq 1$. On a donc $\operatorname{pgcd}(a, n) = a \neq 1$ puis $\phi(n) < (n - 1)$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est donc pas un corps. Réciproquement, supposons que n soit un nombre permier p. Alors tous les nombres compris entre 1 et $p - 1$ sont premiers avec p. On a donc $\phi(p) = p - 1$. Ainsi, tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles sauf 0. □

L'anneau $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ avec p premier est donc un corps que l'on note $\mathbb{F}_p$.

4 Anneaux de matrices

Définition 4.25. 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 4.26. 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 4.27. *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 4.28. 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 4.29. 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 4.30. 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 4.31. *$(M_n(\mathbb{K}), +, \times)$ 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 $(B + C) \times A$. □

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 4.32. 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 4.33. *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 4.34. *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 4.35. *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 4.36. *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 4.37. *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 4.38. *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

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

Ces lois sont biens définies d'après le $a)$ et $b)$. Comme $+_E$ et $\cdot_F$ vérifient les conditions $a), \ldots, h)$ 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 $\vec{u}_1, \ldots, \vec{u}_k$ 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 $i = 1, \ldots, k$. 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 $\mathcal{F} = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n\}$ 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 $E = \text{Vect}_{\mathbb{K}}\{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n\}$.

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 dimesion 1.

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

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

i) si $\mathcal{F} = \{vu_1, ..., \vec{u}_k\}$ 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 $\mathcal{F} = \{vu_1, ..., \vec{u}_k\}$ 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 $\dim E = 2$.

5 Rang d'une matrice

Lemme 5.19. *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 esapce vectoriel.

L'esapce $\mathbb{R}^n$ 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 5.20. 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'esapce des lignes est

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

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 5.21. *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 5.22. 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 5.23. *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 5.24. *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 $c \not\emptyset$ 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 5.25. *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 5.26. 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 5.27. *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 5.28. 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 5.29. *Soit $AX = B$ un système linéaire. Soit X_0 une solution de ce système. Alors l'ensemble S des solutions de ce système est*

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

Proposition 5.30. *Pososns $S' = \{X_0 + Y \mid Y \in \mathrm{Nul}(A)\}$. 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 $S = S'$.*