

ALGÈBRE I

CHAPITRE 1: LES ENSEMBLES



Chapitre I : Les Ensembles



1) Définition:

+ Un ensemble est une collection d'objets vérifiant tous une certaine propriété dite critère d'appartenance à l'ensemble considéré.

+ Les objets formant un ensemble E s'appellent les éléments de E .

Si x est un élément de E : on dit que x appartient à E et on écrit $x \in E$. Dans le cas contraire on écrit $x \notin E$.

Notation: Pour représenter un ensemble E , on écrit entre deux accolades la liste de ses éléments.

Exemples: i) $E = \{1, a, *, T\}$

ii) E l'ensemble des entiers naturels divisant 18;

$$E = \{1, 2, 3, 6, 9, 18\}$$

2) Egalité de deux ensembles:

Définition: on dit que deux ensembles E et F sont égaux et on écrit $E = F$ s'ils sont formés des mêmes éléments.

Exemple: E l'ensemble des solutions réelles de l'équation

$$x^2 - 2 = 0 \quad ; \quad F = \{-\sqrt{2}, \sqrt{2}\}$$

Note: $E = F \Leftrightarrow E \subset F$ et $F \subset E$

3) L'ensemble vide:

Définition: on appelle ensemble vide et on note $\emptyset$ l'ensemble qui ne contient aucun élément ; $\forall x \in \emptyset$

Remarque: i) $E \neq F \Leftrightarrow (\exists x \in E, x \notin F)$ ou $(\exists x \in F, x \notin E)$

ii) $E \neq \emptyset \Leftrightarrow \exists x \in E$

4) Sous-ensembles:

Définition: Soit E et F deux ensembles, on dit que F est un sous-ensemble de E ou que F est une partie

de E ou que F est inclus dans E et on écrit $F \subseteq E$.

Si tout élément de F est un élément de E :

$$F \subseteq E \Leftrightarrow \forall x \in F, x \in E$$

Remarque: $F \not\subseteq E \Leftrightarrow \exists x \in F, x \notin E$

Exemples: i) $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

ii) $\emptyset \subseteq E$

iii) $E \subseteq E$

5) Intersection:

Définition: Soit E et F deux ensembles

On appelle intersection de ces deux ensembles et on

note $E \cap F$ l'ensemble des éléments appartenant à E et à F :

$$E \cap F = \{x / x \in E \text{ et } x \in F\}$$

Exemples: i) $E = \{1, a, 2, b, *\}$; $F = \{1, \Delta, *, 2\}$

$$E \cap F = \{1, 2, *\}$$

ii) $\mathbb{I}$ l'ensemble des entiers naturels impairs et $\mathbb{P}$ l'ensemble des entiers naturels pairs

$$\mathbb{I} \cap \mathbb{P} = \emptyset$$

iii) Soit E un ensemble :

$$E \cap E = E ; E \cap \emptyset = \emptyset ; F \subseteq E \Rightarrow E \cap F = F$$

Remarque: Soit E et F deux ensembles alors on a :

$$E \cap F \subseteq E ; E \cap F \subseteq F$$

Définition: on dit que deux ensembles E et F sont **disjoints** si :

$$E \cap F = \emptyset$$

Exemple: $\mathbb{I}$ et $\mathbb{P}$ sont disjoints.

6) Réunion:

Définition: On appelle réunion ou union de deux ensembles E et F et on note $E \cup F$ l'ensemble des éléments appartenants à E ou à F .

$$E \cup F = \{x / x \in E \text{ ou } x \in F\}$$

Remarque: i) $E \subset E \cup F$

ii) $F \subset E \cup F$

iii) Si $F \subset E \Leftrightarrow E \cup F = E$ ($x \in F \Leftrightarrow x \in E \cup F \Leftrightarrow x \in E$)

7) Partition:

Soit E , et $\mathcal{F}$ un ensemble de partie de E

On dit que $\mathcal{F}$ est une partition de E si :

$$+ \forall x \in \mathcal{F}, x \neq \emptyset$$

$$+ \forall x, y \in \mathcal{F} \text{ si } x \neq y \text{ on a } x \cap y = \emptyset$$

$$+ E = \bigcup_{x \in \mathcal{F}} x$$

Exemples: i) $\mathcal{F} = \{\mathbb{I}, \mathbb{P}\}$ est une partition de $\mathbb{N}$

$$\text{ii) } \mathcal{F} = \{A, B, C\} \text{ où } A = \{3k / k \in \mathbb{N}\}$$

$$B = \{3k+1 / k \in \mathbb{N}\}$$

$$C = \{3k+2 / k \in \mathbb{N}\}$$

Soit $n \in \mathbb{N}$, en effectuant la division Euclidienne de n

$$\text{par } 3 \text{ on a : } n = 3q + r \quad / \quad 0 \leq r \leq 2$$

8) Différence:

Définition: Soit E et F deux ensembles

On appelle différence entre E et F et on note $E - F$

l'ensemble des éléments de E n'appartenant pas à F .

$$E - F = \{x / x \in E \text{ et } x \notin F\}$$

Exemples: i) $E = \{1, a, *, \square\}$
 $F = \{1, a, b, \Delta, T\}$

$$E - F = \{*, \square\}$$

$$F - E = \{b, \Delta, T\}$$

$$\text{on a } E - F \neq F - E$$

ii) Soit E et F deux ensembles

$$E - F = \emptyset \Leftrightarrow E \subset F$$

9) Difference Symétrique:

Définition: Soit E et F deux ensembles

On appelle différence symétrique entre E et F et on note $E \Delta F$ l'ensemble des éléments de E n'appartenant pas à F ou des éléments de F n'appartenant pas à E .

$$E \Delta F = (E - F) \cup (F - E)$$

Exemple: $E = \{1, a, *\}$

$$F = \{1, a, \Delta, T\}$$

$$E \Delta F = \{*, \Delta, T\}$$

Remarques: i) Soit E un ensemble et F une partie de E

$$E \Delta F = E - F$$

ii) Soit E et F deux ensembles

$$E \Delta F = \emptyset \Leftrightarrow E = F$$

$$\text{iii) } E \Delta \emptyset = E$$

$$\text{iv) } E \Delta F = F \Delta E$$

10) Complémentaire:

Définition: Soit E un ensemble et F un sous-ensemble de E , on appelle complémentaire de F par rapport à E et on note

$\overset{F}{\underset{E}{C}}$ l'ensemble des éléments de E n'appartenant pas à F .

$$\boxed{\left[\begin{smallmatrix} F \\ E \end{smallmatrix} \right] = E - F}$$

Exemple: $\left[\begin{smallmatrix} P \\ \mathbb{N} \end{smallmatrix} \right] = \emptyset$; $\left[\begin{smallmatrix} \emptyset \\ \mathbb{N} \end{smallmatrix} \right] = P$

Remarques: i) Soit E un ensemble et $F \subseteq E$: $\left[\begin{smallmatrix} F \\ E \end{smallmatrix} \right] = F$

ii) $\left[\begin{smallmatrix} E \\ E \end{smallmatrix} \right] = \emptyset$

iii) $\left[\begin{smallmatrix} \emptyset \\ E \end{smallmatrix} \right] = E$

iv) Soit E un ensemble vide et F une partie propre de E ($F \neq \emptyset$ et $F \neq E$)

Alors $\left\{ F, \left[\begin{smallmatrix} F \\ E \end{smallmatrix} \right] \right\}$ est une partition de E .

11) Produit Cartésien:

Définition: Soit E et F deux ensembles non vides.

A partir d'un élément x de E et d'un élément y de F on construit un nouveau objet mathématique qu'on note (x, y) et qu'on appelle couple.

L'ensemble des couples d'éléments de E et de F s'appelle le produit cartésien de E et F , on le note $E \times F$ (on lit E croix F).

$$E \times F = \{ (x, y) / x \in E \text{ et } y \in F \}$$

Exemple: $E = \{1, a, *\}$

$F = \{1, \Delta, \square, \top\}$

$$E \times F = \{ (1, 1); (1, \Delta); (1, \square); (1, \top); (a, 1); (a, \Delta); (a, \square); (a, \top); (*, 1); (*, \Delta); (*, \square); (*, \top) \}$$

Remarque: Soit E, F et G trois ensembles non vides.

on convient de poser: $(E \times F) \times G = E \times (F \times G)$

et $\forall x \in E, \forall y \in F, \forall z \in G;$

$$((x, y), z) = (x, (y, z)) = (x, y, z)$$

12) Graphes:

Soit E et F deux ensembles.

On appelle graphe de E vers une partie G de $E \times F$

Exemples: i) $G = \{(x, \frac{1}{x-1}) / x \in \mathbb{N}\}$

G est un graphe de $\mathbb{N}$ vers $\mathbb{Q}$

ii) $E = \{1, a, *\}$

$F = \{\Delta, O, T, L\}$

$G = \{(1, \Delta); (1, O); (*, L)\}$ est un graphe de E vers F .

iii) $E \times F$ est un graphe de E vers F .

$\emptyset$ est un graphe de E vers F

13) Applications:

Définition: Soit E et F deux ensembles non vides

Une fonction de E vers F est la donnée f d'un graphe G de E vers F tel que pour tout élément x de E , il existe **au plus** un élément y de F tel que $(x, y) \in G$

Exemples: $E = \{1, a, *\}$

$F = \{\Delta, O, T, L\}$

* $G_1 = \{(1, \Delta); (1, O); (*, L)\}$

G_1 ne définit pas une fonction E vers F

* $G_2 = \{(1, T); (a, T)\}$

G_2 définit une fonction de E vers F .

Définitions et notations: Soit E, F deux ensembles (f, G) une fonction de E vers F .

i) Soit $x \in E$, s'il existe un élément y de F tel que $(x, y) \in G$, y s'appelle l'image de x par f et on la note $f(x)$.

ii) Soit $y \in F$ on dit qu'un élément x de E est un antécédant de y si $f(x) = y$.

iii) E s'appelle l'ensemble de départ de f et F s'appelle l'ensemble d'arrivée de la fonction f de E vers F se note:

$$f: E \rightarrow F$$

$$x \rightarrow f(x)$$

G s'appelle le graphe de f .

Exemple: $E = \{1, a, *, \Delta\}$

$$F = \{0, b, T, \square, \perp\}$$

$$G = \{(1, 0); (a, T); (\Delta, 0)\}$$

G définit une fonction f de E vers F .

$$\begin{cases} f(1) = 0 & 1 \text{ et } \Delta \text{ sont des antécédants de } 0 \\ f(a) = T & \Rightarrow a \text{ est un antécédent de } T \\ f(\Delta) = 0 & b, \square, \perp \text{ n'ont pas d'antécédent par } f \end{cases}$$

Définition: Soit E et F deux ensembles non vides.

On appelle application de E vers F toute fonction f de E vers F ,

tel que: $\forall x \in E; \exists y \in F, y = f(x)$

SMIA 2

Exemples: i) $f: \mathbb{N} \rightarrow \mathbb{Q}$

$$x \rightarrow \frac{1}{x^2 + 1}$$

est une application de $\mathbb{N}$ vers $\mathbb{Q}$

ii) $f: \mathbb{R} \rightarrow \mathbb{R}$

$$x \rightarrow \frac{1}{x^2 - 1}$$

f est une fonction de $\mathbb{R}$ vers $\mathbb{R}$

mais f n'est pas une application de $\mathbb{R}$ vers $\mathbb{R}$

Notation: Soit E et F deux ensembles

L'ensemble des applications de E vers F se note: F^E

Définitions: Soit E, F deux ensembles et $f \in F^E$

i) Soit $A \in \mathcal{P}(E)$, on appelle image de A par f et on note $f(A)$

l'ensemble $\{f(x) / x \in A\}$

ii) Soit $B \in \mathcal{P}(F)$, on appelle image réciproque de B par f , et on note $f^{-1}(B)$ l'ensemble $\{x \in E / f(x) \in B\}$

iii) on appelle image de f et on note $\text{Im} f$ l'ensemble $f(E)$

Exemple: $E = \{1, a, *, \Delta\}$

$F = \{b, 0, \square, \top, \perp\}$

f l'application de E vers F dont le graphe est:

$$G = \{(1, b); (a, 0); (*, 0); (\Delta, \top)\}$$

$$A = \{1, \Delta\}$$

$$f(A) = \{f(1), f(\Delta)\} = \{b, \top\}$$

$$\begin{aligned} \text{Im} f &= \{f(1), f(a), f(*), f(\Delta)\} \\ &= \{b, 0, \top\} \end{aligned}$$

$$B = \{b, 0\}$$

$$f^{-1}(B) = \{1, a, *\}$$

$$\begin{aligned} C &= \{\square, \perp\} \\ f^{-1}(C) &= \emptyset \end{aligned}$$

Notation: Soit $f \in F^E$ alors pour tout $y \in F$, $f^{-1}(\{y\})$ se note $f^{-1}(y)$

Definition: Soit f une application de E vers F

* On dit que f est injective si pour tout $(x, x') \in E \times E$

$$(x \neq x') \Rightarrow (f(x) \neq f(x'))$$

$$(f(x) = f(x')) \Rightarrow (x = x')$$

* On dit que f est surjective si: $(\forall y \in F), f^{-1}(y) \neq \emptyset$

* On dit que f est bijective si: elle est injective et surjective:

$$(\forall y \in F)(\exists ! x \in E) \quad ; \quad f(x) = y$$

SMIA 2

* Soit f l'application de E vers F définie:

f est injective:

f n'est pas surjective

f n'est pas bijective.

$\mathcal{P}(E \times F)$ = l'ensemble des graphes de E vers F .

Graphe = ensemble de point.

14) Application d'un ensemble vers un ensemble:

Definition: Soit E et F deux ensembles non vides

On appelle fonction de E vers F la donnée f d'un

graphe G de E vers F tel que:

pour tout élément x de E il existe au plus un élément y de F tel que $(x, y) \in G$

Exemples: i) $G = \{(x, \frac{1}{x^2-1}) \mid x \in \mathbb{R}\} \subset \mathbb{R} \times \mathbb{R}$

si $(\forall x \in \mathbb{R}) \quad x \neq \pm 1$, il existe $y \in \mathbb{R} \left(y = \frac{1}{x^2-1}\right)$
tel que $(x, y) \in G$.

G est donc une fonction de $\mathbb{R}$ vers $\mathbb{R}$

ii) $E = \{1, a, *\}$, $F = \{\Delta, \square, \top\}$

$$G = \{(1, \Delta); (1, \top); (*, a)\}$$

G n'est pas une fonction de E vers F .

Notation: Soit (f, G) une fonction de E vers F .

Soit $x \in E$ s'il existe un élément y de F tel que $(x, y) \in G$
 y s'appelle l'image de x par la fonction f et on le
note $f(x)$.

x s'appelle un antécédant de y .

la fonction (f, G) se note

$$f: E \rightarrow F$$

$$x \rightarrow f(x)$$

E s'appelle l'ensemble de départ de f et F l'ensemble
d'arrivée de f .

G s'appelle le graphe de f .

Définition: Soit E et F deux ensembles non vides

On appelle application de E vers F toute fonction f de
 E vers F tel que tout élément de E admet une
image par f .

Exemples: i) $E = \{1, a, *, 0\}$

$$F = \{\Delta, \perp, \square\}$$

$$G = \{(1, \Delta); (a, \perp); (*, \Delta); (0, \perp)\} \in \mathcal{P}(E \times F)$$

G définit une application f de E vers F

$$f(1) = \Delta$$

$$f(a) = \perp$$

$$f(*) = \Delta$$

$$f(0) = \perp$$

1 et $*$ sont deux antécédants de Δ

a et 0 sont deux antécédants de $\perp$

ii) Soit $G = \left\{ \left(x, \frac{1}{x^2+1} \right) / x \in \mathbb{N} \right\} \subset (\mathbb{N} \times \mathbb{Q})$

G définit une application f de $\mathbb{N}$ vers $\mathbb{Q}$

Definitions: Soit E et F deux ensembles non vides

et $f: E \rightarrow F$ une application:

i) Soit A une partie de E on appelle image de A par f

et note $f(A)$ l'ensemble $\{ f(x) / x \in A \}$

$$f(A) = \{ f(x) / x \in A \}$$

($f(E)$ s'appelle l'image de f et on note $\text{Im} f$)

ii) Soit $B \subset F$

On appelle image réciproque de B par f et on

note $f^{-1}(B)$ l'ensemble $\{ x \in E / f(x) \in B \}$

Exemple:

$$E = \{ 1, a, *, 0 \}$$

$$F = \{ \Delta, b, \square, \top, \perp \}$$

f l'application de E vers F dont le graphe est: $G = \{ (1, \Delta); (a, b); (*, b); (0, \top) \}$

$$A = \{ 1, * \}$$

$$f(A) = \{ f(1), f(*) \}$$

$$f(A) = \{ 1, b \}$$

$$B = \{b\}$$

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

$$= \{a, * \}$$

$$\text{Im} f = f(E) = \{f(1), f(a), f(*), f(o)\}$$

$$= \{\Delta, b, T\}$$

$$f^{-1}(\{L\}) = \emptyset, \quad f^{-1}(F) = E$$

Notation: Soit $f: E \rightarrow F$ une application

Pour tout élément y de F , $f^{-1}(\{y\})$ se note tout simplement $f^{-1}(y)$

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

L'ensemble des applications de E vers F se note F^E

Définition: Soit f une application de E vers $F \Rightarrow F^E$

i) On dit que f est **injective** si pour tout $(x, x') \in E \times E$
 $(x \neq x') \Rightarrow (f(x) \neq f(x'))$
 $(f(x) = f(x')) \Rightarrow (x = x')$

ii) On dit que f est **surjective** si: $\forall y \in F : f^{-1}(y) \neq \emptyset$

iii) On dit que f est **bijjective** si elle est injective et surjective: $\forall y \in F, \exists! x \in E, y = f(x)$

Exemples: i) $E = \{1, 2, 3, 4\}$

$$F = \{a, b, c, d, e\}$$

Soit f l'application de E vers F définie

$$\text{par: } f(1) = a, \quad f(2) = b, \quad f(3) = c, \quad f(4) = d$$

f est injective, f n'est pas surjective

f n'est pas bijective.

ii) $E = \{1, 2, 3, 4\}$, $F = \{a, b, c\}$

soit $g: E \rightarrow F$

$g(1)=a$; $g(2)=b$; $g(3)=b$, $g(4)=c$

g n'est pas injective , g est surjective

iii) $E = \{1, 2, 3, 4\}$, $F = \{a, b, c, d\}$

$h: E \rightarrow F$

$h(1)=a$; $h(2)=b$; $h(3)=a$; $h(4)=c$

h n'est pas injective

h n'est pas surjective



iv) $E = \{1, 2, 3, 4\}$

$F = \{a, b, c, d\}$

$i: E \rightarrow F$

$i(1)=a$; $i(2)=b$; $i(3)=c$; $i(4)=d$

i est injective , i est surjective
donc i est bijective

Definition : Soit E, F, G trois ensemble : $f \in F^E$ et $g \in G^F \Rightarrow F \Rightarrow G$

On appelle composé de f et g et on note $g \circ f$ (grand f) l'application de E vers G définie pour toute élément x de E par:

$$g \circ f(x) = g(f(x))$$

$$\begin{array}{ccccc} E & \xrightarrow{f} & F & \xrightarrow{g} & G \\ & & & & \uparrow \\ & & & & g \circ f \end{array}$$

$$x \mapsto f(x) \mapsto g(f(x))$$

Exemple: $f: \mathbb{N} \rightarrow \mathbb{R}$
 $x \mapsto \frac{1}{x^2+1}$



$g: \mathbb{R} \rightarrow \mathbb{R}$
 $x \mapsto 2x+1$

$g \circ f: \mathbb{N} \rightarrow \mathbb{R}$

$g \circ f(x) = g(f(x))$
 $= g\left(\frac{1}{x^2+1}\right) = 2\left(\frac{1}{x^2+1}\right) + 1$

$g \circ f(x) = \frac{x^2+3}{x^2+1}$

Théorème: Soit E, F, G trois ensembles $f \in F^E$ tel que $g \in G^F$

si f et g sont bijectives alors $g \circ f$ est bijective.

Démonstration: i) Soit x et x' deux éléments de E tels que :

$g \circ f(x) = g \circ f(x')$

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

comme g est injective on a :

$f(x) = f(x')$

comme f est injective on a : $x = x'$

donc $(g \circ f)$ est injective

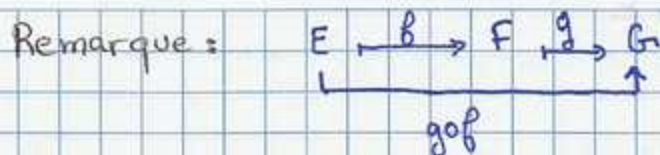
ii) Soit $z \in G$

Comme g est surjective, il existe un élément de F tel que $g(y) = z$

Comme f est surjective, il existe un élément $x \in E$ tel que $f(x) = y$

on déduit que $g \circ f(x) = g(f(x)) = g(y) = z$

$\Rightarrow g \circ f$ est surjective.



alors : i) f et g injectives $\Rightarrow$ $g \circ f$ injective

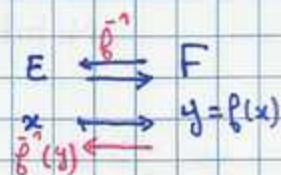
ii) f et g surjectives $\Rightarrow$ $g \circ f$ surjective

Définition: Soit E, F deux ensembles et $f \in F^E$

si f est bijective on appelle application réciproque de f et on note f^{-1}

l'élément de E^F définie par :

$$\begin{aligned}
 \forall y \in F: \quad f^{-1}(y) &= x \\
 (\Leftrightarrow) \quad y &= f(x)
 \end{aligned}$$



Exemple: $E = \{1, 2, 3, 4\}$, $F = \{a, b, c, d\}$

$$f: E \rightarrow F \quad ; \quad f^{-1}: F \rightarrow E$$

$$f(1) = a, \quad f(2) = b, \quad f(3) = c, \quad f(4) = d$$

$$f^{-1}(a) = 1, \quad f^{-1}(b) = 2, \quad f^{-1}(c) = 3, \quad f^{-1}(d) = 4$$

Théorème: $f \in F^E$ et $g \in G^F$

si f et g sont bijectives alors :

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$



15) Permutation d'un ensemble :

Définition: Soit E un ensemble non vide

On appelle permutation de E toute application bijective de E vers E

L'ensemble des permutations de E se note S_E .

Exemple: $E = \{1, 2, 3, 4, 5, 6\}$

$$f: E \rightarrow E$$

$$f(1) = 2$$

$$f(2) = 3$$

$$f(3) = 4$$

$$f(4) = 5$$

$$f(5) = 6$$

$$f(6) = 1$$

$$f \in S_E$$



Notation: Pour tout $n \in \mathbb{N}^*$, on désigne par $\mathbb{N}_n$ l'ensemble $\{1, 2, \dots, n\}$. L'ensemble des permutations de $\mathbb{N}_n$ est noté S_n .

Un élément $\sigma \in S_n$ se note :

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

Exemple: Les éléments de S_3

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

$$\tau_{23} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\tau_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

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

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

$$\tau_{13} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

alors $S_3 = \{e, \tau_{12}, \tau_{13}, \tau_{23}, \sigma, \psi\}$

Remarque: on a $\text{Card}(S_n) = n!$

Définition: On dit qu'un élément $\sigma \in S_n$ est une transposition de N_n s'il existe deux éléments distincts i et j de N_n tels que :

$$\sigma(i) = j$$

$$\sigma(j) = i$$

$$\sigma(k) = k, \quad \forall k \notin \{i, j\}$$

Lorsqu'il en est ainsi σ se note τ_{ij} ou τ_{ji}

Exemple: Les transpositions de N_3 sont τ_{12}, τ_{13} et τ_{23} .

Théorème: Pour toute transposition τ_{ij} de N_n on a :

$$\tau_{ij} \circ \tau_{ij} = e$$

e : étant la permutation identité de N_n

$$(e(k) = k, \quad \forall k \in N_n)$$

Démonstration: Soit $k \in N_n$

- Si $k = i$ on a :

$$\tau_{ij} \circ \tau_{ij}(i) = \tau_{ij}(\tau_{ij}(i)) = i$$

- Si $k = j$ on a :

$$\tau_{ij} \circ \tau_{ij}(j) = j$$

- Si $k \notin \{i, j\}$ on a :

$$\begin{aligned} \tau_{ij} \circ \tau_{ij}(k) &= \tau_{ij}(\tau_{ij}(k)) \\ &= \tau_{ij}(k) \\ &= k \end{aligned}$$

Théorème: Pour tout $\sigma \in S_n$, il existe des transpositions $\tau_1, \tau_2, \tau_3, \dots, \tau_k$ de S_n tel que $\sigma = \tau_1 \circ \tau_2 \circ \tau_3 \circ \dots \circ \tau_k$.

Démonstration: On raisonne par récurrence sur n :

i) Pour $n=2$ on a $S_2 = \{e, \tau_{12}\}$

$$\tau_{12} \circ \tau_{12} \circ \tau_{12} = \tau_{12}$$

ii) Hypothèse de récurrence on suppose le résultat vrai pour n .

iii) Soit $\sigma \in S_{n+1}$

Deux cas sont possibles:

* 1^{er} cas: $\sigma(n+1) = n+1$

Soit $\varphi: \mathbb{N}_n \rightarrow \mathbb{N}_n$ définie par

$$\varphi(i) = \sigma(i)$$

$$\varphi \in S_n$$

D'après l'hypothèse de récurrence, il existe des transpositions $t_1, t_2, t_3, \dots, t_k$ de S_n tel que: $\varphi = t_1 \circ t_2 \circ t_3 \circ \dots \circ t_k$

Pour tout i ($1 \leq i \leq k$)

Soit $\tau_i: \mathbb{N}_{n+1} \rightarrow \mathbb{N}_{n+1}$ définie par

$$\tau_i(j) = \begin{cases} t_i(j) & \text{si } 1 \leq j \leq n \\ n+1 & \text{si } j = n+1 \end{cases}$$

τ_i est une transposition de $\mathbb{N}_{n+1}$

Soit $j \in \mathbb{N}_{n+1}$ si $j = n+1$ on a:

$$\tau_1 \circ \tau_2 \circ \dots \circ \tau_k(n+1) = n+1 = \sigma(n+1)$$

$$\text{Si } j \in \mathbb{N}_n, \text{ on a } \tau_1 \circ \tau_2 \circ \dots \circ \tau_k(j) = t_1 \circ t_2 \circ \dots \circ t_k(j) = \varphi(j) = \sigma(j)$$

$$\text{donc } \tau_1 \circ \tau_2 \circ \dots \circ \tau_k = \sigma$$



SMIA 2

$$\forall \sigma \in S_n$$

$$\exists z_1, \dots, z_k \text{ transposé}$$

$$\sigma = z_1 \circ \dots \circ z_k$$

Il existe deux cas : 1^{er} cas : $\sigma(n+1) = n+1$

2^{ème} cas : $\sigma(n+1) \neq n+1$

Soit $q \in \mathbb{N}_n$ tel que :

$$\sigma(q) = n+1$$

et Soit $\varphi = \sigma \circ z_{q, n+1}$

$$\begin{aligned} \text{on a : } \varphi(n+1) &= \sigma(z_{q, n+1}) \\ &= \sigma(q) \\ &= n+1 \end{aligned}$$

donc d'après le 1^{er} cas, il existe des transpositions $t_1, t_2, t_3, \dots, t_k$ de S_{n+1} telles que : $\varphi = t_1 \circ t_2 \circ \dots \circ t_k$

$$\Rightarrow \sigma = t_1 \circ t_2 \circ \dots \circ t_k \circ z_{q, n+1}$$

$\Rightarrow \sigma$ est la composée de transpositions de S_{n+1}

Définition : On dit que deux ensembles E et F sont équipotents s'il existe une application bijective de E vers F

Exemple : Soit $E = \{*, T, \leq\}$

$$f: E \rightarrow \mathbb{N}_3$$

définition : $f(*) = 1$

$$f(T) = 2$$

$$f(\leq) = 3$$

f est bijective $\Rightarrow E$ et $\mathbb{N}_3$ sont équipotents.