M103 — § 0 Arithmétique

$\mathbb{N}$ = { 1, 2, 3, 4, 5, ..., 13, 14, 15, ..., 23, 24, ..., 3016, ..., 774 006 73533 }

0.1 def : $n \in \mathbb{N}$ est dit premier si il n'a pour diviseur que deux diviseurs, c'est à dire

si $\begin{cases} k \mid n \\ k \neq 1 \end{cases} \Rightarrow k = 1$ ou $k = n$

0.2 def : Soit $k, n \in \mathbb{N}$. On dit que "k divise n" s'il existe un nombre m tel que $km = n$

Notation $k \mid n$

0.2.5 On étend la définition 0.1 également aux entiers négatifs : $-2 \mid 14$; $3 \mid -27$

$\{-n \mid n \in \mathbb{N}\}$

$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}$

0.3 Exemple : l'ensemble des diviseurs de $n = 12$ est :

$\{1, 2, 3, 4, 6, 12\}$

0.4 Attention : $n = 1$ n'est pas un nombre premier

0.5 **Proposition** : Pour tout $n \in \mathbb{N}$ il existe une décomposition

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_r$$

les p_i sont premiers, et $r \geq 0$

N.B : un produit de 0 facteurs est égal à 1 par convention

Preuve : * Supposons n premier, on définit $p_1 = n$ et on obtient l'énoncé $n = p_1$ (ici $n = 1$)

* Supposons n non premier, Selon 0,2, il existe $m, k \in \mathbb{N}$ tel que $k.m = n$ avec $2 \leq k, m \leq n-1$

alors, par récurrence on peut supposer que l'énoncé (S) est vrai pour k et m, c'est à dire $k = p'_1 \times \cdots \times p'_{r'}$ et $m = p''_1 \cdot \cdots \cdot p''_{r''}$ où p' et p'' sont premiers et $r' \geq 0$ et $r'' \geq 0$

donc $n = k.m = (p'_1 \cdots p'_{r'}) \cdot (p''_1 \cdots p''_{r''}) = p'_1 \cdot p'_1 \cdots p'_{r'}$

$p_i := p'_i \quad (1 \leq i \leq r')$

$p_j := p''_{j-r'}$

où $r = r' + r''$

□

0.6 **Remarque** : La décomposition $n = p_1 \cdots p_r$ dans la prop 0,5 est unique à un changement d'ordre parmi les p_i "près" ...

Question : c'est qui le plus grand nombre premier ?

0.7 : Soit p premier, soit $n \in \mathbb{N}$. Alors si $p \mid n$, dans ce cas $p \nmid (n+1)$

M103

preuve : $p \mid n \Rightarrow n = k \cdot p$, $k \in \mathbb{N}$

Supposons que si $p \mid n$, $p \mid (n+1)$
dans ce cas, il existe m tel que $n+1 = m \cdot p$
$(m \in \mathbb{N})$

$$1 = (n+1) - n = pm - pk = p(m-k)$$
$$\neq 1 \quad \neq 0$$

donc $p(m-k) \geq 2$ donc $1 \geq 2$ donc absurde
donc si $p \mid n$, $p \nmid (n+1)$

0.8 Il y a un nombre infini de nombres premiers $n \in \mathbb{N}$
En particulier, il n'y a pas de plus grand nombre premier

Preuve : Supposons que l'ensemble de premiers soit fini : $\{2, 3, 5, \dots p_M\}$

On définit $n = 2 \cdot 3 \cdot 5 \cdot \dots \cdot p_n$
On observe que tout premier $p \mid n$

On considère $n+1$ et on applique le lemme 0.7 pour déduire que $p \nmid (n+1)$

~~Donc n+1 est un nombre premier plus grand que~~

Donc pour $n+1 = p_1 \cdot \dots \cdot p_k$ (prop 0.5)
tout p_i sont différents des p

et donc $\forall p_i > p_M$ donc p_M n'est pas le plus grand nombre premier

0,9 Attention : dans la preuve 0,8, on ne peut pas conclure que $n+1$ est premier.

0.10 Collection d'énoncé arithmétique pour discuter

A_1) si $M = \{n_1, n_2, n_3 \dots\}$, $n \in \mathbb{N}$ tel que :

(a) $1 \in M$

(b) $\forall n \in \mathbb{N} \Rightarrow n+1 \in M$

Alors $M = \mathbb{N}$

A_2) Pour tout $\begin{cases} M \subset \mathbb{N} \\ M \neq \emptyset \end{cases}$ il existe un m_0 tel que

pour tout $m \in M$ on a $m_0 \leq m$

m_0 est le plus petit élément de M

B_1) Soit $k, m, n \in \mathbb{N}$

$k \mid m$ et $m \mid n \Rightarrow k \mid n$

B_2) Soit $k, m, n \in \mathbb{N}$

$k \mid m \Rightarrow k \mid m.n$

M103

C1) La décomposition $n = p_1 \cdot \ldots \cdot p_k$ (0.5) est unique, à permutation des facteurs près

O_1) Pour tout $n \in \mathbb{N}$, n pair ≥ 2, il existe des premiers p_1, p_2 tel que :

conjecture de Goldbach →

$$n = p_1 + p_2$$

O_2) Il existe une infinité de premiers p tels $p+2$ est également premier (p et $p+2$ sont dits "jumeaux premiers")

Conjecture des jumeaux premiers →

M103

§ 1 Ensembles

1.1 Exemples

(a) $\{1, 2, 3\}$

(b) $\{2, 3, 8, 17\}$

(c) $\{\square, \circ, \triangle\}$

(d) $\{2, 4, 6, 8, 10, 12, \ldots\}$

(e) $\{n \mid n \in \mathbb{N}, 2 \mid n\}$

Notons : (a), (b), (c) ensembles finis
(d), (e) ensembles infinis.

1.2 Remarques

(1) Un ensemble est une "boîte mathématique"
La propriété importante d'un ensemble est qu'il "contient" des objets mathématiques :

Ex : $1 \in \{1, 2, 3\}$, $2 \in \{1, 2, 3\}$, $4 \notin \{1, 2, 3\}$

On note pour A ensemble $a \in A$ ou $A \ni a$
$a \notin A$ ou $A \not\ni a$

(2) Un ensemble est bien défini, pour tout objet x et tout ensemble A on a $\begin{cases} a \in A \text{ ou } A \notin A \\ \text{mais jamais } a \in A \text{ et } a \notin A \\ \text{et toujours un des 2} \end{cases}$

(3) Un ensemble ne peut contenir un élément qu'une fois :
$\{1, 2, 3 \mid 1 = 2\} = \{1, 2, 3\}$

Ex : l'ensemble des valeurs de la suite $x_1 = 1, x_2 = 0, x_3 = 1, \ldots$ est $\{0, 1\}$

(4) Deux ensembles sont égaux si et seulement si les éléments de l'un sont contenus dans l'autre, et réciproquement.

c'est à dire, soit A, B deux ensembles.

$$A = B \iff \begin{cases} A \subset B \\ B \subset A \end{cases} \iff \begin{cases} x \in A \Rightarrow x \in B \\ x \in B \Rightarrow x \in A \end{cases}$$

En particulier, il n'y a pas d'ordre dans les éléments

1.3) Problèmes potentiels

(a) Problème pratique : Des fois c'est difficile à juger si deux objets sont les mêmes ou non

ex : $\square \in \{\square, \circ, \triangle\}$?

Solution : il faut demander des spécifications regardant l'ensemble donné.

(b) Problème de base ; Exemple de B. Russel (version Lusig)

$V := \{h \mid h$ homme, h habité à Hamlet$\}$

$V \ni b$ = le barbier de Hamlet

Tradition de Hamlet. Tout homme de Hamlet, soit se rase lui même, soit il va chez b se faire raser mais pas les deux.

MI203

$V_b = \{ l \in V \mid l \text{ se rase lui même} \}$

$b \in V_b$?

Aucune réponse n'est logiquement compatible avec les hypothèses.
On ne peut pas définir V_b

1.4.1) Notations :
Soient A, B des ensembles

A, B

: définition

(a) $A \subset B :\Leftrightarrow$ Si $x \in A$, alors $x \in B$

(b) $A \cap B := \{ x \mid x \in A \text{ et } x \in B \}$

(c) $A \cup B := \{ x \mid x \in A \text{ ou } x \in B \}$

(d) $A \setminus B$ $(= A - B)$ $:= \{ x \mid x \in A \text{ et } x \notin B \}$

(e) $A \Delta B = \{ x \mid x \in A \setminus B \text{ ou } x \in B \setminus A \}$

Δ différence symétrique (ou exclusif)

(f) Soient A, B contenus dans un ensemble universel X

$\complement_X(A) = \{ x \mid x \notin A \ (x \in X) \}$

1.5) Définition : Soient A, B ensembles. On définit le produit cartésien

$A \times B = \{ (a, b) \mid a \in A, b \in B \}$

Attention : $(a, b) = (a', b') \Rightarrow \begin{cases} a = a' \\ b = b' \end{cases}$

En particulier : $(1, 0) \neq (0, 1)$

1.6) L'ensemble des parties

Pour tout ensemble A, on définit :

$\mathcal{P}(A) = \{ A' \mid A' \subset A \}$

↳ "l'ensemble des parties de A"

Q : Si A contient n éléments, alors combien d'éléments contient $\mathcal{P}(A)$?

1.7) Ensembles remarquables

(a) L'ensemble vide : $\{\} = \emptyset$

(b) $\mathbb{N}$ = entiers naturels
$\mathbb{Z}$ = entiers relatifs
$\mathbb{Q}$ = rationnels
$\mathbb{R}$ = réels
$\mathbb{C}$ = complexes

1.8) Les "familles"

On appelle : Un élément a peut faire partie d'un ensemble A qu'une fois.

Par contre une "famille" $(x_i)_{i \in I}$ peut comporter la même valeur plusieurs fois.

(b) Les familles finies se notent alternativement comme n-uplets

$(x_i)_{i \in \{1,2,3\}} = (a, b, c) \neq (b, a, c)$ sauf si $a = b$

où $x_1 = a$; $x_2 = b$; $x_3 = c$

1.9) Règles (voir 1.4)

Pour tout A, B, C :

(a) $A \cap B = B \cap A$
$A \cup B = B \cup A$ } commutativité

(b) $A \cap (B \cap C) = (A \cap B) \cap C$
$A \cup (B \cup C) = (A \cup B) \cup C$ } associativité

(c) $A \cup \emptyset = A$
$A \cap \mathcal{X} = A$ } éléments neutres

$\mathcal{X}$: ensemble universel

(d) $A \cup A^{-1} = \emptyset$
$A \cap A^{-1} = \mathcal{X}$ } "inverse"

A^{-1} existe-t-il ?

(e) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ } distributivité

(f) $A \Delta B = (A \cup B) \setminus (A \cap B)$
$= (A \setminus B) \cup (B \setminus A)$

On vérifie : $A \Delta B = B \Delta A$

$(A \Delta B) \Delta C = A \Delta (B \Delta C)$

$A \Delta \emptyset = A$

$A \Delta A = \emptyset$

Associativité, élément neutre, et inverse, donc $\mathcal{X}$ est un groupe par rapport à l'opérateur Δ

Si en plus on a commutativité, c'est un "groupe commutatif" ou "groupe abélien"

$A \cap (B \Delta C) = (A \Delta B) \cap (A \Delta C)$

§ 2 → ?

§ 3 Fonctions (applications) et Relations

3.(-1) Non définition:

Pour définir une relation, on a besoin de deux choses :

1) Deux ensembles A et B

2) Propriété $\mathcal{P}$ entre un élément $a \in A$ et $b \in B$

Exemple :

(1) A = garçons d'une classe
B = filles d'une classe
$\mathcal{P}(a,b)$ = "a est amoureux de b"

(2) $A = B = \mathbb{N}$
$\mathcal{P}(a,b)$ = "$a \mid b$"

3.0) Exemple de relations R_i $(i = 1, 2, 3, 4)$

(a) $n, m \in \mathbb{Z}$: $n \, R_1 \, m \Leftrightarrow n \mid m$

(b) $n, m \in \mathbb{Z}$: $n \, R_2 \, m \Leftrightarrow \exists p$ premier tel que $p \mid n$ et $p \mid m$

(c) $n, m \in \mathbb{N}$: $n \, R_3 \, m \Leftrightarrow n \leq m$

(d) $a, b \in A$ $a \, R_4 \, b \Leftrightarrow a = b$

3.1) Définition : Soit R une relation entre A et B. On définit le "graphe" de R comme

$A \times B \supset R = \{(a,b) \mid a \, R \, b\}$

(b) En effet, une relation R entre A et B est un sous ensemble, $A \times B \subset R$, et
$a \, R \, b \Leftrightarrow (a,b) \in R$

3.1.1) Composition de relations

Soient $R \subset A \times B$ et $R' \subset B \times C$
On définit la composition :
$R' \circ R \subset A \times C$ par :
$(a,c) \in R' \circ R \Leftrightarrow \exists b \in B$ tel que: $(a,b) \in R$
$(b,c) \in R'$

3.1.3) Propriétés des relations
Soit $R \subset A \times B$ une relation.
On définit :

(i) R "unique à gauche" si $a \, R \, b$ et $a' R b \Leftrightarrow a = a'$

(ii) R "——— à droite" si $a \, R \, b$ et $a \, R \, b' \Leftrightarrow b = b'$

iii) R "total à gauche" si $\forall a \in A, \exists b \in B : a \, R \, b$

iv) R "total à droite" si $\forall b \in B, \exists a \in A : a \, R \, b$

3.1.4) Exemples

Soient $m, n \in \mathbb{N}$. $m R_1 n \Leftrightarrow m \mid n$, $m \neq n$, $m \geq m'$ si $m' \mid n$ et $n \neq m'$

On observe que R satisfait (i)(iii) mais pas (ii), ni (iv) (à cause de $m = 1$)

Donc R_1' définie comme R_1^{-1} sur $\mathbb{N} - \{1\}$

$R_1' : \mathbb{N} - \{1\} \to \mathbb{N}$

$n \to m$ m est donc le plus grand diviseur de n différent de n

Donc R_1' non injective mais surjective

3.1.5) Exemples

A quelconque, $\mathcal{R} = Id_A$ donné par $Id_A \subset A \times A$

$Id_A = \{(a, a') \mid a = a'\}$

↳ ok pour tous les 3.1.3)

3.1.8) Déf: Une relation $\mathcal{R} \subset A \times B$ est appelé "application" (ou "fonction")
si et seulement si $\mathcal{R}$ satisfait (ii) et (iii) de 3.1.3)

On écrit $\mathcal{R} : A \longrightarrow B$ et $\mathcal{R}(a) = b \iff a \mathcal{R} b$

3.2) Définition :
Soit $f : A \to B$ une application

(i) f "injective" $\iff \forall a \neq a' \Rightarrow f(a) \neq f(a') \iff$ (i) ↳ 3.1.3)

(ii) f "surjective" $\iff \forall b \in B, \exists a \in A$ tel que $f(a) = b$

(iii) f "bijective" $\iff f$ injective et surjective

(iv) a est "préimage de b" $\iff f(a) = b \iff b$ est image de a

A est "domaine" de f ou "ensemble préimage" ou "ensemble de départ"

B est "ensemble image" de f ou "ensemble d'arrivée"

$B \supset f(A) = \{b \mid \exists a \in A \text{ tel que } f(a) = b = Im(f)\}$
$A \supset A'$, $f(A') = \{b \in B \mid \exists a' \in A', f(a') = b\}$

$B \supset B'$, $f(B') = \{a \in A \mid f(a) \in B'\}$

v/ La "restriction" de $f : A \to B$
à $A' \subset A$ est noté $f|_{A'}$ et donné par

$f|_{A'} : A' \to B$
$a' \to f(a')$

Lemme → 3.2.5) Soient $f : A \to B$, $g : B \to C$
Alors
(a) Si $g \circ f$ surjective $\Rightarrow$ g surjective
(b) Si $g \circ f$ injective $\Rightarrow$ f injective

Preuve : (TD)

3.3) Proposition : $f : A \to B$ est bijective
$\Leftrightarrow \exists f' : B \to A$ si seulement si :
$f' \circ f = id_A$ et $f \circ f' = id_B$

Preuve :
$\Leftarrow$ $f' \circ f = id_A$ injective $\xrightarrow{(3.2.5)}$ f injective } donc
$f \circ f' = id_A$ surjective $\longrightarrow$ f surjective } f bijective

$\Rightarrow$ f bijective $\Rightarrow$ f satisfait (i), (ii), (iii) et (iv) dans (3.1.3)

Donc f définit une application $f' = f^{-1}$

$f' : B \to A$
$b \to a$

On vérifie, $\forall a \in A$, $f' \circ f(a) = f'(f(a)) = f'(b) = a$
donc $f' \circ f = id_A$

$\forall b \in B$, $f \circ f'(b) = f(a) = b$
donc $f \circ f' = id_B$

□

3.3.1) Remarque : une loi interne "$*$" (quelconque) définie sur un ensemble A est une application :

$$\begin{aligned} * : A \times A &\longrightarrow A \\ (a, a') &\longrightarrow a * a' \end{aligned}$$

3.2.2) Définition : (importante)
Soient $(A, \circ)$ et $(B, *)$ deux ensembles munis d'une loi interne. Une application $f : A \to B$ est dite un "morphisme" par rapport à "$\circ$" et "$*$" si et seulement si, $\forall (a, a') \in A^2$,
$f(a \circ a') = f(a) * f(a')$

$\Leftrightarrow$ "l'image du produit est égal au produit des images" (somme) (somme)

3.3.4) Exemple : $f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \longmapsto & e^x \end{array}$

est un morphisme de $(\mathbb{R}, +)$ à $(\mathbb{R}, \cdot)$

$f(x_1 + x_2) = e^{x_1 + x_2} = e^{x_1} \cdot e^{x_2} = f(x_1) \cdot f(x_2)$

3.4.1) Définition. Soit $\mathcal{R} \subset A \times A$

(a) $\mathcal{R}$ "réflexive" $\Leftrightarrow \forall a \in A$, $a \mathcal{R} a$

(b) $\mathcal{R}$ "symétrique" $\Leftrightarrow \forall a, a' \in A$, $a \mathcal{R} a' \Leftrightarrow a' \mathcal{R} a$

(c) $\mathcal{R}$ "transitive" $\Leftrightarrow \forall a, a', a'' \in A$, si $a \mathcal{R} a'$ et $a' \mathcal{R} a''$ alors $a \mathcal{R} a''$

(d) $\mathcal{R}$ "antisymétrique" $\Leftrightarrow$ $a \mathcal{R} b$ et $b \mathcal{R} a \Rightarrow a = b$

(e) $\mathcal{R}$ satisfait "comparabilité" $\Leftrightarrow \forall a, a' \in A$ $a \mathcal{R} a'$ ou $a' \mathcal{R} a$

3.4.2) Exemple

1) M ensemble, $A = \mathcal{P}(M)$ (ensemble des parties de M : $\{A' \subset M\}$, et $\mathcal{R}$ donné par "$\subset$"

satisfait (a), (c), (d)

Chapitre 4 : Ensembles infinis

4.0) Soient A et B ensembles finis.
Les trois suivants sont équivalents

(1) B est "plus grand ou égal à" A

(2) $\exists f : A \longrightarrow B$ injective

(3) $\exists f : B \longrightarrow A$ surjective

(4) $\#B \geq \#A$

Preuve :
Exemple : soit $A = \{1, 2, \dots, m\}$
$B = \{1, 2, \dots, n\}$

$(m, n \in \mathbb{N})$ on observe :

$A \Leftrightarrow n \geq m$ $\Leftrightarrow$ $A \xrightarrow{f \text{ injectif}} B$: $k \longrightarrow \begin{cases} k \text{ si } k \leq n \\ m \text{ si } k > m \end{cases}$

car $\#A = m$
et $\#B = n$ $\Leftrightarrow \exists B \longrightarrow A$ (f surjectif)

(voir TD4) je remarque que dans ce cas :
(2) $\Rightarrow$ (4) et (3) $\Rightarrow$ (4)

On note : A fini $\Leftrightarrow \exists$ une bijection :

$$\ell_A : A \to \{1, \dots, \#A\}$$

↳ "compter"

Donc tout se ramène au cas spécial ($\subset \mathbb{N}$)

4.1) Deux ensembles A et B (finis ou infinis) ont le même "cardinal"

$|A| \Leftrightarrow \exists\ f : A \to B$ bijective

4.1.5) Exemples :

$\mathbb{N}$ et $\mathbb{Z}$ ont le même cardinal

$$\mathbb{Z} \to \mathbb{N}$$

$$k \to \begin{cases} -2k & , k < 0 \\ 2k+1 & , k \geq 0 \end{cases}$$

↳ bijective donc ok

4.1.8) Définition : tout ensemble A qui a le même cardinal que $\mathbb{N}$ est dit "dénombrable"

4.2) Th : $\#\mathbb{N} \neq \#\mathbb{R}$

Preuve : (1) : trivial , (3) : trivial

(2) : $a \sim_f a' \Leftrightarrow f(a) = f(a')$

3.6) Exemple : $f : \mathbb{N} \to \mathbb{Z}$

$$x \to \begin{cases} 0 & \text{si } x \text{ pair} \\ 1 & \text{si } x \text{ impair} \end{cases}$$

$$\mathbb{N} \to \mathbb{N} / \sim_f \to \{0, 1\} \subset \mathbb{Z}$$

$$\{\{2, 4, 6, \dots\}, \{1, 3, 5, \dots\}\}$$

3.7) Application importante :

$\forall\, m \in \mathbb{N}$, on définit $\mathcal{R}_m \subset \mathbb{Z} \times \mathbb{Z}$

$\forall\, n_1, n_2 \in \mathbb{Z}$, $n_1 \mathcal{R}_m n_2 \Leftrightarrow \exists\, k \in \mathbb{Z}$

tel que $n_2 = n_1 + k.m$

$\Leftrightarrow m \mid n_1 - n_2$

Note : $\mathcal{R}_m$ est une relation d'équivalence (vérifier)

on note $n_1 \equiv n_2$

ou $n_1 \equiv n_2 \bmod m$

$$\mathbb{Z} / \overset{(m)}{\equiv} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$$

$$= \mathbb{Z}/(m)$$

$$= \mathbb{Z}_m$$

$$\overline{n} = \{ \ldots, n-2m, n-m, n, n+m, n+2m, \ldots \}$$

L'importance de ces ensembles quotients dérivera de l'absurde que $\overline{n_1}+\overline{n_2} = \overline{n_1+n_2}$ et $\overline{n_1}\cdot\overline{n_2} = \overline{n_1 \cdot n_2}$ } est bien définit

Si $m = p$ premier $\Rightarrow \mathbb{Z}/(p)$ est un corps

2) $A = \mathbb{R}$, $\mathcal{R}$ donné par "$\leq$" satisfait (a), (c), (d), (e)

3) $A = \mathbb{R}$, $\mathcal{R}$ donné par "$<$" satisfait (c), (d)

3.4.5) Définition : $A \times A \supset \mathcal{R}$, on suppose que $\mathcal{R}$ satisfait (a), (c) et (d) , alors c'est un ordre "partiel" sur A.

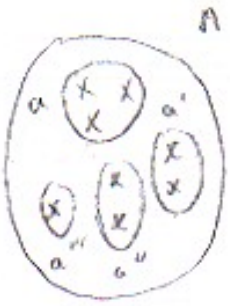
si $\mathcal{R}$ satisfait (a), (c), (d), (e) , alors c'est un ordre "total" sur A

si $\mathcal{R}$ satisfait (a), (b) , et (c) alors c'est une relation "d'équivalence" sur A

3.4.8) Exemple : Soit $f : A \to B$ application. Alors $A, A \supset \mathcal{R}_f$ donné par : $a \mathcal{R}_f a'$
$\Leftrightarrow a \sim_f a'$
$\Leftrightarrow f(a) = f(a')$

3.4.9) Lemme : Soit A ensemble avec relation d'équivalence "$\sim$".
$\forall\, a \in A$, on définit $[a] = \{a' \in A \mid a' \sim a\}$
("relation d'équivalence de a"). Les sous-ensembles de A (c'est à dire les éléments de $\mathcal{P}(A)$) donnés comme classe d'équivalence satisfait :

$[a] \cup [a'] \cup [a''] \cup \dots = A$



(a) $[a] \neq \emptyset$

(b) $[a] \cap [a'] = \begin{cases} \emptyset \\ [a] = [a'] \end{cases}$ $\forall a, a' \in A$

(c) $\bigcup_{a \in A} [a] = A$

On définit $A/\sim \; = \{[a] \mid a \in A\} \subset \mathcal{P}(A)$

("ensemble quotient" associé à "$\sim$")

Exemple : $A = \{a, b, c, d, e, f\}$

$f \; \mathcal{R} \; a \sim b \sim c \; \mathcal{R} \; d \sim e \; \mathcal{R} \; f$

$A/\sim \; = \{\{a, b, c\}, \{d, e\}, \{f\}\}$

Exercice : preuve du Lemme du 3.4.5

3.5) Proposition : Toute application $f : A \to B$ se décompose :

$$A \longrightarrow A/\sim_f \longrightarrow f(A) \xrightarrow{c} B$$

$$a \longrightarrow [a] \; (= [a']) \longrightarrow f(a) \; (= f(a')) \longrightarrow f(a)$$

(1) surjective (2) bijective (3) injective

Preuve : (absurde) On suppose qu'il existe $f : \mathbb{N} \to \mathbb{R}$ bijective

On construit $x \in \mathbb{R} \setminus f(\mathbb{N})$ de la façon suivante :

$\mathbb{N}$ | $\mathbb{R}$

1 | $0,\boxed{0}000\ldots$
2 | $17,3\boxed{3}23\ldots$
3 | $3,14\boxed{1}59\ldots$

$\rightarrow +1 \,[10]$

$x = 0,142$

On est certain que $f(n) \neq x \quad \forall n \in \mathbb{N}$
$f(\mathbb{N}) \subsetneq \mathbb{R} \setminus f(\mathbb{N})$ puisque le n-ième chiffre sera toujours différent.
On ne peut pas trouver x dans l'ensemble $\mathbb{R}$ de départ

Sauf : $1,0000\ldots = 1$ donc si on aura
$0,9999\ldots = 1$ non 9, on met un 0

Donc on change un peu la méthode !

et ça marche □

4.3) Les cardinals possibles sont

Remarque →

(a) linéaires ("totale") ssi
$\Leftrightarrow \forall A, B$, $A \leq B$ ou $B \leq A$

(b) pas bornée : $\forall$ cardinal $\exists$ un autre cardinal strictement plus grand

$A < B \iff \nexists\, f : A \longrightarrow B$ surjective
$\iff \exists\, g : B \to A$ injective.

Chapitre 5 : Composition d'applications et "permutations"

5.1) (a) On définit $\forall$ ensemble A l'application

$$\begin{aligned} id_A \quad A &\to A \\ a &\to a \end{aligned}$$

(b) $\forall f : A \to B$ on a $f \circ id_A = f$
$id_A \circ f = f$

Les doublets se comptent algébriquement comme des "éléments neutres"

(c) $\forall$ $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$

on a $h \circ (g \circ f) = (h \circ g) \circ f$

on écrit $h \circ g \circ f$

(d) $\forall f : A \to B$ bijective $\Rightarrow \exists$ une "inverse" $f^{-1} : B \to A$ et : $f \circ f^{-1} = id_B$
et $f^{-1} \circ f = id_A$

(e) Cas particuliers :

$A = B$ $\Rightarrow$ $B_{ij}(A) = \{ f : A \to A \mid f$ bijective $\}$

est un groupe par rapport à sa loi interne "$\circ$" (non abélien)

En général, $A \xrightarrow{f} A \xrightarrow{g} A$ différent de $A \xrightarrow{g'} A \xrightarrow{f} A$

Prop 5.2) : (voir précédent)

5.3) Pour le reste du chapitre, on considère le cas spécial où $B = A$ ensembles finis particuliers $A = \{1, 2, \dots, n\}$

On note $B_{ij}(A) = S_n$ "groupe symétrique"

et on note $S_n \ni \sigma : \sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$

groupe symétrique (B) permutation

Ex : $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \in S_n$ donné par

$\{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$

L'élément "la bijection d'un ensemble fini", ou "groupe symétrique", est une "permutation" des éléments de l'ensemble

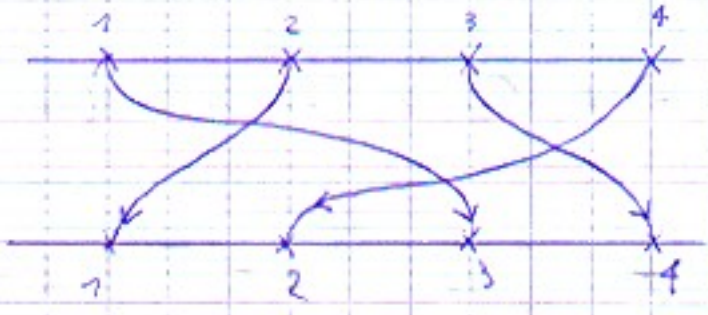
$$id_A = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

Composition :

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

Représentation géométrique

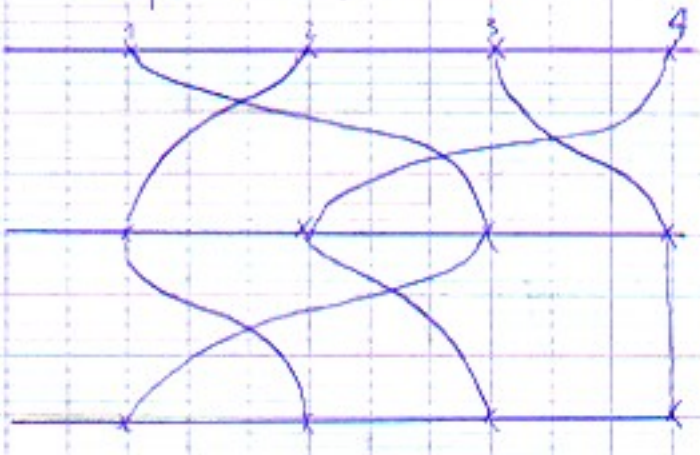


σ

à éviter dans le diagramme : pas d'intersection de plus de 2 brins :  non !

le brin ne revient pas  non !

Composition :



σ

τ

5.4.5) Lemme : $\# S_n = n!$

5.5) Transposition (définition)

$$\tau_{i,j} = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ 1 & \dots & j & \dots & i & \dots & n \end{pmatrix}$$

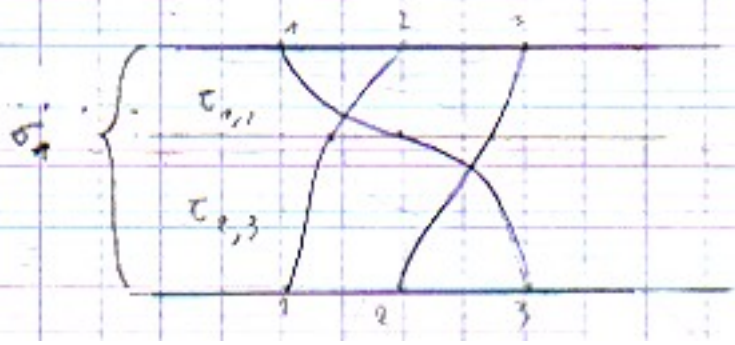
5.6) Proposition :
permutations $\forall \sigma \in S_n$ se décompose (non uniquement) comme produit de transpositions

$$\sigma_n = \tau_{n-1,\, i_{n-1}} \circ \dots \circ \tau_{i_2, i_1} \circ \tau_{i_1, i_0}$$

Preuve (exemple) :

$$\sigma_1 = \tau_{2,3} \circ \tau_{1,2} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{pmatrix}$$

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



5.7) Remarque - Définition

(a) Donnée $\sigma \in S_n$, on considère une "tresse" représentant σ.
On sait qu'toute autre tresse représentant σ peut bien, avec un autre nombre de points d'intersection, mais la différence est toujours paire.

(b) On obtient une invariante de σ, dite "signature", définie par :

$$sign(\sigma) = (-1)^{\text{nombre de points d'intersection dans la tresse de } \sigma}$$

5.8) Proposition :

La signature est un homomorphisme

$$sign : S_n \longrightarrow \{-1, 1\} \quad \text{(groupe multiplicatif)}$$
$$\sigma \longrightarrow sign(\sigma)$$

c'est à dire $\forall\ \sigma_1, \sigma_2 \in S_n$: $sign(\sigma_1 \circ \sigma_2) = sign(\sigma_1) \circ sign(\sigma_2)$

Preuve : $\#\text{intersection}(\sigma_1 \circ \sigma_2) = \#\text{intersections}(\sigma_1) + \#\text{intersection}(\sigma_2)$

donc $\#\cap(\sigma_1 \circ \sigma_2) = \#\cap\sigma_1 + \#\cap\sigma_2$

donc $\Rightarrow (-1)^{\#\cap(\sigma_1 \circ \sigma_2)} = (-1)^{\#(\cap\sigma_1 + \#\cap\sigma_2)}$

$$(-1)^{\#(\sigma_1 \circ \sigma_2)} = (-1)^{\#\cap\sigma_1} \cdot (-1)^{\#\cap\sigma_2}$$