

T.D. M51.

Emmy DUCLOS.

Rd E, F des ens.

⑤ Une application de E vers F ,
 notée $f: E \rightarrow F$, c'est la donnée
 pr. tt. $x \in E$, d'un élmt $f(x) \in F$.

- E est appelé ens de définition de f
- F est appelé ens d'arrivée

D) Soit $A \subseteq E$, $B \subseteq F$,
l'image de A par f, notée $f(A)$, est
 $f(A) = \{ f(a) \text{ pour } a \in A \}.$

L'image réciproque de B par f , notée $f^{-1}(B)$ est

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

④ La restriction de f à A , notée $f|_A$ est l'application

T.D. M51. Emmanuèle DUCLOS. ① La corestriction de f à B , notée $f|_B^B$ est l'application $f|_B^B : f(B) \rightarrow B$ $x \mapsto f(x)$.

Ex 1: Sei $f: E \rightarrow F$ eine applicat. $A \subseteq E, C \subseteq F$.
 $B \subseteq E, D \subseteq F$.

a) Mg A $\subseteq f^{-1}(f(A))$ (lorsque f est injective).

\rightarrow mit $x \in A$, alors $f(x) \in f(A)$ dc $x \in f^{-1}(f(A))$.

On a bien rangé $A \subseteq f^{-1}(f(A))$.

\rightarrow Since f is injective, $\exists x \in f^{-1}(f(A))$, $\exists y \in A$ tq $f(x) = f(y)$.

\hat{e} is not injective, on a $x = y$.

D'où $x \in A$, donc $f^{-1}(f(A)) \subseteq A$.

Par double inclusion : $A = f^{-1}(f(A))$.

G) Mq $f(f^{-1}(C)) \subseteq C$ ($\begin{array}{l} \text{d'après laq} \\ f \text{ est surjective} \end{array}$) d) Mq $f(A \cup B) = f(A) \cup f(B)$.
 soit $y \in f(f^{-1}(C))$ alors $\exists x \in f^{-1}(C)$ tq $y = f(x)$
 $\Leftrightarrow y \in f(A \cup B) \Leftrightarrow \exists x \in A \cup B$ tq $y = f(x)$
 $\Leftrightarrow (\exists x \in A \mid y = f(x)) \text{ ou } (\exists x \in B \mid y = f(x))$
 $\Leftrightarrow y \in f(A) \text{ ou } y \in f(B)$
 $\Leftrightarrow y \in f(A) \cup f(B)$.

Comme $x \in f^{-1}(C)$, on a $f(x) \in C$, de $y \in C$.
cel $f(f^{-1}(C)) \subseteq C$.
 Supposons f est surjective, soit $y \in C$,
 alors comme f est surjective, $\exists x \in E \mid y = f(x)$.
 Puisque $y \in C$, on a $x \in f^{-1}(C)$ & de
 $y \in f(f^{-1}(C))$.

On a dc mqé lorsque f est surjective,
 $C \subseteq f(f^{-1}(C))$.

& p double-inclusion: $C = f(f^{-1}(C))$.

d) Mq $f(A \cap B) \subseteq f(A) \cap f(B)$ ($\begin{array}{l} \text{de égalité basque} \\ f \text{ est injective} \end{array}$)
 soit $y \in f(A \cap B) \Rightarrow \exists x \in A \cap B \mid y = f(x)$
 comme x est à la fois dans A et B , on a
 $y = f(x) \in f(A)$ et $y \in f(B)$.

Donc $y \in f(A) \cap f(B)$; d'où $f(A \cap B) \subseteq f(A) \cap f(B)$
 Supp f injective, soit $y \in f(A) \cap f(B)$ alors
 $y \in f(A)$, de $\exists x \in A$ tq $y = f(x)$
 $y \in f(B)$, de $\exists x' \in B$ tq $y = f(x')$
 $\exists f$ est injective & $f(x) = f(x')$; on a $x = x'$.
 (E) $x \in A \cap B$; d'où $y \in f(A \cap B)$, & dc
 $f(A) \cap f(B) \subseteq f(A \cap B)$. Par double inclusion,
 $f(A) \cap f(B) \subseteq f(A \cap B)$. Par double inclusion,
 $f(A \cap B) = f(A) \cap f(B)$.

$$e) \text{ Mq } f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$$

$$x \in f^{-1}(C \cup D) \Leftrightarrow f(x) \in C \cup D$$

$$\Leftrightarrow f(x) \in C \text{ ou } f(x) \in D$$

$$\Leftrightarrow x \in f^{-1}(C) \text{ ou } x \in f^{-1}(D)$$

$$\Leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D)$$

$$\text{D'où } f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D).$$

$$f) \text{ Mq } f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$$

$$x \in f^{-1}(C \cap D) \Leftrightarrow f(x) \in C \cap D$$

$$\Leftrightarrow f(x) \in C \text{ et } f(x) \in D$$

$$\Leftrightarrow x \in f^{-1}(C) \text{ et } x \in f^{-1}(D)$$

$$\Leftrightarrow x \in f^{-1}(C) \cap f^{-1}(D)$$

$$\text{D'où } f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$$

voir ex 2 ③

e) Mq $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.
 $x \in f^{-1}(C \cup D) \Leftrightarrow f(x) \in C \cup D$

$$\Leftrightarrow f(x) \in C \text{ ou } f(x) \in D$$

$$\Leftrightarrow x \in f^{-1}(C) \text{ ou } x \in f^{-1}(D)$$

$$\Leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D)$$

D'où $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.

f) Mq $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$

$$x \in f^{-1}(C \cap D) \Leftrightarrow f(x) \in C \cap D$$

$$\Leftrightarrow f(x) \in C \text{ et } f(x) \in D$$

$$\Leftrightarrow x \in f^{-1}(C) \text{ et } x \in f^{-1}(D)$$

$$\Leftrightarrow x \in f^{-1}(C) \cap f^{-1}(D)$$

D'où $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$

Ex: Que dire de l'ens $F(E, F)$ lorsque $E = \emptyset$ ou $F = \emptyset$!

• $E \neq \emptyset$ mais $F = \emptyset$

$$\boxed{\text{M1}} |F(E, F)| = |F|^{|E|} = 0^{|E|} = 0 \text{ et } F(E, F) = \emptyset$$

card(-) := 1.1

M2 soit $f \in F(E, F)$, soit $x \in E$, alors $f(x) \in F = \emptyset$

Donc $\forall x \notin F$, $F(E, F) = \emptyset$.

• $E = \emptyset$

$$(|F(E, F)| = |F|^{|E|} = |F|^0 = 1)$$

$$\bullet f(x) = \frac{1}{\sqrt{1+x^2}} \rightarrow \mathcal{D}_f = \mathbb{R}. \quad (\text{on n'impose q' f})$$

Définir une applica $\emptyset \rightarrow F$, c'est donner $\forall n \in \emptyset$, une image $f(n)$. Comme le \emptyset ne contient pas d'elt, on peut faire le faire & d'une seul façon. $F(\emptyset, F)$ ne contient de qu'un sol elt.

voir ex2 ③

Ex 4 Soit E un ensemble. (TH) Cantor.

Mq \nexists appli surjective $f: E \rightarrow \mathcal{P}(E)$

Indic°: considérez $X = \{x \in E \mid x \notin f(x)\}$.

Supposons l'absurde qu'il existe $f: E \rightarrow \mathcal{P}(E)$ surjective.

Considérons $X = \{x \in E \mid x \notin f(x)\}$

Puisque f est surjective, $\exists x \in E$ tq $x = f(a)$.

Est-ce que $a \in X$?

\rightarrow supp $a \in X$ alors $a \in f(a)$. de $a \notin X$. $\textcircled{2}$)

\rightarrow supp $a \notin X$ alors $a \notin f(a)$ dc $a \in X$. $\textcircled{01}$)

On a donc les 2 cas une absurdité.

dc f ne peut pas être surjective.

Ex 5 : (TH) Cantor - Bernstein

a) $G: \mathcal{P}(E) \rightarrow \mathcal{P}(E)$ f croissante.

$M = \bigcup_{A \in S} A$ où $S = \{A \in \mathcal{P}(E) \mid A \subset G(A)\}$

Mq $M \subset G(M)$, soit $x \in M$ alors
 $\exists A \in S$ tq $x \in A$.

Donc $A \subset G(A)$, et $x \in G(A)$.

dc $x \in \bigcup_{A \in S} G(A) = G(M)$ d'où $M \subset G(M)$.

Mq $G(M) \subset M$:

soit $G(x) \in G(A)$ $\forall A \in S$.

on sait que $A \subset G(A)$, dc comme G est croissante $G(A) \subset G^2(A) = G(G(A))$.

Donc $G(A) \in S$. Donc $G(x) \in \bigcup_{A \in S} A = M$

D'où $G(M) \subset M$.

Par double inclusion :

$M = G(M)$ | c'est bien un point fixe.

suite Thm Cantor-Bernstein

On ut mg Thm Cantor-Bernstein.

On a déjà mgé si $G: \mathcal{P}(E) \rightarrow \mathcal{P}(F)$ est alors elle a un point fixe M.

b) $f: E \rightarrow F$, $g: F \rightarrow E$ 2 injects.

Considérons $G: \mathcal{P}(E) \rightarrow \mathcal{P}(E)$ $\stackrel{\text{Mg est}}{\text{et}}$ $\stackrel{G}{\text{et}}$

$$A \mapsto E \setminus g(F \setminus f(A)).$$

soit $A \subset B \subset E \Rightarrow f(A) \subset f(B)$.

$$F \setminus f(A) \supset F \setminus f(B)$$

$$g(F \setminus f(A)) \supset g(F \setminus f(B))$$

$$E \setminus g(F \setminus f(A)) \subset E \setminus g(F \setminus f(B))$$

$$G(A) \subset G(B)$$

De f. & est ↑.

Alors @, G possède un point fixe $M \in \mathcal{P}(E)$.

$$M = E \setminus g(F \setminus f(M))$$

$$\text{ou encore } E \setminus M = g(F \setminus f(M))$$

g. $F \setminus f(M) \rightarrow E$ est une inject & son image est $E \setminus M$, c'est dc une biject $F \setminus f(M) \rightarrow E \setminus M$.

On pt alors définir

$$h: E \longrightarrow F$$
$$x \longmapsto \begin{cases} f(x) & \text{si } x \in M \\ (g|_{E \setminus M})^{-1}(x) & \text{si } x \notin M \end{cases}$$

• h est injective.

est injective par hypothèse.

$(g|_{F \setminus f(M)})^{-1}$ est bijective, dc ep injective.

si $x \in M$ & $y \in E \setminus M$ alors $h(x) = f(x) \in M$,

$$h(y) = (g|_{E \setminus M})^{-1}(y) \in F \setminus f(M).$$

Donc $h(x) \neq h(y)$. h est bien injective

• f est surjective:

$$\begin{aligned} h(E) &= h(M \cup E \setminus M) = h(M) \cup h(E \setminus M) \\ &= f(M) \cup (g|_{E \setminus M})^{-1}(M) \\ &= f(M) \cup (F \setminus f(M)) \end{aligned}$$

$$\boxed{h(E) = F}$$

h est bien surjective.

⑤

On a donc bien construit une bijet $f: E \rightarrow F$.

Rélation d'équivalence

Quo

- ④ Une relation R sur un ensemble E , c'est une pie.
On note $x R y \Leftrightarrow (x, y) \in R$.
 $\Rightarrow =, \leq, <, \dots$

⑤ Une relation d'équivalence est une relation vérifiant 3 propriétés:

- 1) Réflexivité: $\forall x \in E \quad x R x$
- 2) Symétrie: $x R y \Rightarrow y R x, \forall (x, y) \in E^2$
- 3) Transitivité: $x R y \wedge y R z \Rightarrow x R z, \forall (x, y, z) \in E^3$

⑥ Une partition d'un ensemble E , c'est une famille $(E_i)_{i \in I}$ de sous-ensembles de E telle que

1. $i \neq j$ alors $E_i \cap E_j = \emptyset$
2. $\bigcup_{i \in I} E_i = E$

⑦ On appelle R une relation d'équivalence sur E . La classe d'équivalence $[x]$ de x est l'ensemble de tous les éléments $y \in E$ tq $x R y$.
On note E/R l'ensemble des classes d'équivalence de E .

⑧ Si $x R y$, x et y ont la même classe.

Les classes forment une partition de E .

Pour montrer que f est injective, il suffit de montrer $(x, y) R (x', y') \Rightarrow f(x, y) = f(x', y')$.
On a $x - y = x' - y' \Rightarrow x + y' = x' + y$.

⑨ Donc f est injective.

Ex 9 Soit R relation sur \mathbb{N}^2 définie par $(x, y) R (x', y') \Leftrightarrow x + y' = x' + y$

- a) Montrer R est une relation d'équivalence.
 - 1) Réflexivité: $x + y = x + y$ de $(x, y) R (x, y)$.
 - 2) Symétrie: Supposons $(x, y) R (x', y')$, alors $x + y' = x' + y$ de $x' + y = x + y'$ d'où $(x', y') R (x, y)$.
 - 3) Transitivité: Supposons $(x, y) R (x', y')$ et $(x', y') R (x'', y'')$ alors $x + y = x' + y'$ et $x' + y'' = x'' + y'$.
De $x + y'' = x + y' + y'' = x + y - y' + y'' = x'' + y' + y - y'$.
 $x + y'' = x'' + y$ de $(x, y) R (x'', y'')$

Donc R est une relation d'équivalence.

b) Déterminer la bijection entre \mathbb{N}^2/R et \mathbb{Z}

$$\begin{aligned} f: \frac{\mathbb{N}^2}{R} &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto x - y \end{aligned}$$

Voyons que f est bien définie.

Si $(x, y) R (x', y')$, alors $x + y' = x' + y$ de $x - y = x' - y'$
Si f ne dépend pas du choix d'un représentant, elle est bien définie.

Soit $(x, y), (x', y') \in \mathbb{N}^2$ tq $f(x, y) = f(x', y')$

Pour montrer f est injective, il suffit de montrer $(x, y) R (x', y') \Rightarrow f(x, y) = f(x', y')$.

On a $x - y = x' - y' \Rightarrow x + y' = x' + y$.

Soit $k \in \mathbb{Z}$.

1. si $k \geq 0$, $k = f(k, 0)$
2. si $k < 0$, $k = f(0, -k)$

Donc f est surjective.

Ex 10 Soit $f: E \rightarrow F$ une application.

On définit la relation R sur E par
 $x R y \Leftrightarrow f(x) = f(y)$.

C'est une relation d'équivalence.
 f se factorise alors en

$$E \xrightarrow{p} E/R \xrightarrow{f} \text{Im } f \xrightarrow{i} F$$

1. p : la projection $E \rightarrow E/R$ (surjective)
2. f est bijective.
3. i est l'inclusion $\text{Im } f \hookrightarrow F$ (injective)

Cette factorisation $f = i \circ \bar{f} \circ p$ est appelée décomposition canonique de f .

trouver un antécédent à deux fois

Ex 13 Déterminer la décomposition canonique de l'application $f: \mathbb{R} \rightarrow \mathbb{C}$ définie par $f(x) = e^{ix}$ pour $x \in \mathbb{R}$.

On définit la relation d'équivalence R sur \mathbb{R} par
 $x R y \Leftrightarrow f(x) = f(y)$.

Alors $x R y \Leftrightarrow e^{ix} = e^{iy} \Leftrightarrow e^{i(x-y)} = 1 \Leftrightarrow x - y \in 2\pi\mathbb{Z}$. De $\mathbb{R}/R = \mathbb{R}/2\pi\mathbb{Z}$

De plus, $\text{Im } f = \{e^{inx} \mid n \in \mathbb{R}\}$
 $= \{z \in \mathbb{C} \mid \lg z \mid = 1\}$
 $= \mathbb{U}$ ou $S(0, 1)$

Donc la décomposition canonique est

$$\begin{aligned} \mathbb{R} &\xrightarrow{p} \mathbb{R}/2\pi\mathbb{Z} \xrightarrow{\bar{f}} \mathbb{U} \xrightarrow{i} \mathbb{C} \\ x &\mapsto n + 2\pi\mathbb{Z} \longmapsto f(n) = e^{in} \longmapsto z \end{aligned}$$

(7)

Ex PT soit $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}^*$ l'appl
 $f(k,n) = (2k+1)2^n + (k,n) \in \mathbb{N} \times \mathbb{N}$.

R Ens dénombrable = Ens de m° cardinal que \mathbb{N} ,
 ie un ens en biject° avec \mathbb{N} .

Ens au plus dénombrable = ens dénombr au fini.

a) Mg f est bijective.

$$f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}^*$$

$$(k,n) \mapsto (2k+1)2^n$$

sait $m \in \mathbb{N}^*$, d'après le TH de décomp°
 en facteurs premiers, $\exists!$ décomp°

$$m = \prod_{p \text{ premier}} p^{d_p}$$

$$m = 2^{d_2} \times \prod_{\substack{p \text{ premier} \\ p \neq 2}} p^{d_p}$$

impair

$$m = f\left(\frac{\prod_{p \text{ premier}, p \neq 2} p^{d_p} - 1}{2}, d_2\right)$$

comme la décomp° en facteurs premiers
 de m est uniq, c'est son uniq antécédent.

Donc $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}^*$ est bijective.

$$\text{com: } \prod_{p \text{ premier}} (2k+1)p^{d_p} - 1 \leftrightarrow k = \frac{\prod_{p \text{ premier}} p^{d_p} - 1}{2}$$

b) et $\mathbb{N} \times \mathbb{N}$ est dénombr

$$\begin{aligned} \text{On a la biject° } & \mathbb{N}^* \rightarrow \mathbb{N} \\ & n \mapsto n-1 \end{aligned}$$

dc $\mathbb{N} \times \mathbb{N}$ est de m° card que \mathbb{N}^* &
 de de \mathbb{N} , dc $\mathbb{N} \times \mathbb{N}$ est dénombr.

c) Mg PR \mathbb{N}^m est dénombr.

On sait que \mathbb{N} et \mathbb{N}^2 est dénombr.

On appelle $m \geq 3$ & \mathbb{N}^{m-1} dénombr.

$$\mathbb{N}^m = \mathbb{N}^2 \times \mathbb{N}^{m-2} \xrightarrow{\text{biject°}} \mathbb{N} \times \mathbb{N}^{m-2} = \mathbb{N}^{m-1}$$

dc \mathbb{N}^m est dénombr.

sait $f: \mathbb{Z} \rightarrow \mathbb{N}$ biject°.

alors on a la biject°

$$f^m: \mathbb{Z}^m \rightarrow \mathbb{N}^m$$

$$(z_1, \dots, z_m) \mapsto (f(z_1), \dots, f(z_m))$$

et \mathbb{Z}^m est, tout comme \mathbb{N}^m , dénombr.

NB $f: \mathbb{Z} \rightarrow \mathbb{N}$

$$k \mapsto \begin{cases} 2k & \text{si } k \geq 0 \\ -2k-1 & \text{si } k < 0. \end{cases}$$

Ex 8 Mg ens \mathbb{Q} des rationnels est dénombrable.

→ On va construire l'inject° $\mathbb{Q} \hookrightarrow \mathbb{N}$
 & $\mathbb{N} \hookrightarrow \mathbb{Q}$.

• $f: \mathbb{N} \rightarrow \mathbb{Q}$ l'inject° naturelle $n \mapsto n$

• i chg rationnels, on pl \Leftrightarrow une uniq écriture
 fractionn° p/q &

- p & q premiers entre ean
- $q > 0$.

(3)

On pt définir $g: \mathbb{Q} \hookrightarrow \mathbb{Z}$

$$\frac{p}{q} \mapsto (p, q)$$

q est bien injective.

Comme \mathbb{Z}^2 est dénombrable (ex 17), \exists une biject°
 $t: \mathbb{Z}^2 \rightarrow \mathbb{N}$
 et de $h: \mathbb{Q} \hookrightarrow \mathbb{N}$ est injective.

D'aprè le TH Cantor-Bernstein, \exists une biject°
 $\mathbb{N} \rightarrow \mathbb{Q}$.

Donc \mathbb{Q} est dénombrable. (au en biject° + \mathbb{N}).

(8)

E*61 But Mg \exists bij. entre $P(\mathbb{N})$ & \mathbb{R}

a) Mg une pte de \mathbb{R} contenant un intervalle ouvert non vide est un bijct \mathbb{R} .

stat $A \subset \mathbb{R}$ une pte contenant $[a, b] \subset$

Gn a une inject A $\hookrightarrow \mathbb{R}$ naturelle
 $x \mapsto n$

Gn a la bijct:

$$\text{arctan}: \mathbb{R} \rightarrow]-\frac{\pi}{2}, \frac{\pi}{2}[$$

\exists bijct affine $f:]-\frac{\pi}{2}, \frac{\pi}{2}[\rightarrow [a, b]$

Donc $f \circ \text{arctan}: \mathbb{R} \rightarrow A$ est injective.

Gn a 2 injcts $A \rightarrow \mathbb{R}$ & $\mathbb{R} \rightarrow A$,
de p le Th de Cantor-Bernstein:
on a une bijct.

6) Mg $\phi: P(\mathbb{N}) \rightarrow \mathbb{R}$, $\phi(A) = \sum_{m=0}^{\infty} \frac{\chi_A(m)}{3^m}$

où χ_A f caract de A (on) bien def & injective

$\phi: P(\mathbb{N}) \rightarrow \mathbb{R}$

$$A \mapsto \sum_{m=0}^{\infty} \frac{\chi_A(m)}{3^m}$$

$$x_m, \left| \frac{\chi_A(m)}{3^m} \right| \leq \frac{1}{3^m}$$

$$\text{Qc } \sum_{m=0}^{\infty} \left| \frac{\chi_A(m)}{3^m} \right| \leq \sum_{m=0}^{\infty} \frac{1}{3^m} = \frac{1}{1-\frac{1}{3}} = \frac{3}{2}$$

La suite est abs. \textcircled{O} , dc ϕ est bien def.

Sups $A \neq B$.

sont m_0 l+petit entier tq $\chi_A(m_0) \neq \chi_B(m_0)$
qu'il suffit à permute A & B, on pt m supposer
 $m_0 \in A$, $m_0 \notin B$.

$$\phi(A) - \phi(B) = \sum_{m=0}^{\infty} \frac{\chi_A(m) - \chi_B(m)}{3^m}$$

$$\phi(A) - \phi(B) = \sum_{m=0}^{\infty} \frac{\chi_A(m) - \chi_B(m)}{3^m}$$

$$= \frac{1}{3^{m_0}} + \sum_{m=m_0+1}^{\infty} \frac{\chi_A(m) - \chi_B(m)}{3^m}$$

$$\geq \frac{1}{3^{m_0}} - \sum_{m=m_0+1}^{\infty} \frac{1}{3^m} \geq \frac{1}{3^{m_0}} - \frac{1}{3^{m_0+1}} \sum_{m=0}^{\infty} \frac{1}{3^m}$$

$$\geq \frac{1}{3^{m_0}} - \frac{1}{3^{m_0+1}} \times \frac{3}{2} \geq \frac{1}{2 \times 3^{m_0}} > 0.$$

Donc $\phi(A) \neq \phi(B)$.

ϕ est bien une injct de P(N) dans R.

ϕ est unif $\phi: P(\mathbb{N}) \hookrightarrow \mathbb{R}$.

où les dyadiq $(x_n)_{n \in \mathbb{N}}$ d'un nbs réel
 $x \in [0, 1]$ est def récurrem^t p

$$x_0 = \lfloor 2n \rfloor \quad \& \quad x_{n+1} = \left\lfloor 2^{n+1} \left(2n - \sum_{k=0}^n \frac{x_k}{2^k} \right) \right\rfloor$$

Mg c'est une suite de 0 & 1 tq

$$x = \sum_{n=0}^{\infty} \frac{x_n}{2^{n+1}}$$

et $[0, 1] \hookrightarrow P(\mathbb{N})$, est injctive.
 $x \mapsto \{n \in \mathbb{N}, x_n = 1\}$

soit $x \in [0, 1]$, on déf. (x_n) p

$$\begin{cases} x_0 = \lfloor 2n \rfloor \\ x_{n+1} = \lfloor 2^{n+1} (2x - \sum_{k=0}^n \frac{x_k}{2^k}) \rfloor \end{cases}$$

On va mon PR:

$$P_m: x_m \in \{0, 1\} \quad \& \quad x'_m = n - \sum_{k=0}^m \frac{x_k}{2^{k+1}} \in E_0, \frac{1}{2^{m+1}}[$$

① $x \in [0, 1]$; $x_n \in \{0, 1\}$ dc $x_0 = \lfloor 2x \rfloor \in \{0, 1\}$.

$$x'_0 = n - \frac{\lfloor 2x \rfloor}{2} = \frac{2n - \lfloor 2x \rfloor}{2} \in [0, \frac{1}{2}]$$

Dc P_0 est vérifiée.

② Sup P_m & my P_{m+1} .

$$2n - \sum_{k=0}^m \frac{x_k}{2^k} = 2x'_m \in [0, \frac{1}{2^m}] \text{ p HDR.}$$

$$\text{Dc } 2^{m+1} \left(2n - \sum_{k=0}^m \frac{x_k}{2^k} \right) \in [0, 1].$$

$$\text{dc } x_m = \left\lfloor 2^{m+1} \left(2n - \sum_{k=0}^m \frac{x_k}{2^k} \right) \right\rfloor \in \{0, 1\}$$

$$x'_{m+1} = x - \sum_{k=0}^{m+1} \frac{x_k}{2^{k+1}} = x - \frac{x_{m+1}}{2^{m+2}}$$

$$= x - \frac{\lfloor 2^m x_m \rfloor}{2^{m+2}}$$

$$= \frac{2^{m+2} x_m - \lfloor 2^{m+2} x_m \rfloor}{2^{m+2}} \in [0, \frac{1}{2^{m+2}}[$$

On a donc bien $\mathbb{P}(\mathbb{N})$.

D'où $(x_n)_{n \in \mathbb{N}}$ est une suite de 0 & de 1.

De plus, $x'_m \in [0, \frac{1}{2^{m+1}}[$ de $x'_m \xrightarrow[m \rightarrow \infty]{} 0$

$$\text{de } n - \sum_{k=0}^m \frac{x_k}{2^{k+1}} \xrightarrow[m \rightarrow \infty]{} 0, \text{ i.e. } \boxed{x = \sum_{k=0}^m \frac{x_k}{2^{k+1}}}$$

soit $\Psi: [0, 1] \rightarrow \mathcal{P}(\mathbb{N})$

$$x \mapsto \{n \in \mathbb{N}, x_n = 1\}$$

alors $x = \Psi(x) = \Psi(y)$ implique $x_n = 1 \Leftrightarrow y_n = 1$.

Comme $(x_n), (y_n)$ est à l'IMO à $\{0, 1\}$, cela signifie que les 2 suites ont les mêmes val.^{es}. ②

$$\text{Donc } x = \sum_{m=0}^{\infty} \frac{x_m}{2^{m+1}} = \sum_{m=0}^{\infty} \frac{y_m}{2^{m+1}} = y.$$

Donc $\Psi: [0, 1] \hookrightarrow \mathcal{P}(\mathbb{N})$ est injective.

d) On a une injec $\phi: \mathcal{P}(\mathbb{N}) \hookrightarrow \mathbb{R}$.

On a aussi l'injeco $\psi: [0, 1] \hookrightarrow \mathcal{P}(\mathbb{N})$ & on a montré en a) que $[0, 1]$ est un bijet à \mathbb{R} .

On peut de appliquer le Th de Cantor-Bernstein pr décliner qu'il existe \exists un bijet entre $\mathcal{P}(\mathbb{N})$ & \mathbb{R} .

e) D'après ex4, il n'y a pas de bijet entre \mathbb{N} & $\mathcal{P}(\mathbb{N})$. Il n'existe pas non plus de bijet entre \mathbb{N} & \mathbb{R} .

\mathbb{R} est indénombrable.

T.D 2 - Groupes

* Un ① monogène est un groupe G engendré par un seul élé, i.e. $\exists g \in G$ tq

$$G = \{g^k, k \in \mathbb{Z}\}$$

s'il est fini, on dit que c'est un groupe cyclique. \exists alors $n \in \mathbb{N}^*$ tq G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

* Si il est infini, $\mathbb{Z} \rightarrow G$ est un isomorphisme. $k \mapsto g^k$ (isomorphie de ① bijets)

$$\text{si pour } \forall g \neq 1, g^2 \neq 1, g^3 \neq 1, g^4 = 1, \\ g^{4k+1} = g^1 ; g^{4k+2} = g^2$$

On a un isomorphisme: $\mathbb{Z}/4\mathbb{Z} \rightarrow G$

$$k \mapsto g^k$$

→ Elle n'existe: on cherche $(a, b) \in \mathbb{R}_+^* \times \mathbb{R}$ tq

$$(a, b) \cdot (c, d) = (a, b)$$

Donc $\begin{cases} ac = a \\ ad + b = b \end{cases} \Leftrightarrow \begin{cases} c = 1 \\ d = 0 \end{cases}$ car $a \in \mathbb{R}_+^*$

E.1 Mg $\mathbb{R}_+^* \times \mathbb{R}$ munie de la loi $(a, b) \cdot (c, d) = (ac, ad+b)$ est un groupe.

→ Stabilité: soit $(a, b), (c, d) \in \mathbb{R}_+^* \times \mathbb{R}$

$$\text{on a } a, c > 0 \text{ dc } ac \in \mathbb{R}_+^*$$

$$\text{de } (a, b) \cdot (c, d) \in \mathbb{R}_+^* \times \mathbb{R}$$

$$\begin{aligned} \text{Assoiativité: } & (a, b) \cdot (c, d) \cdot (e, f) \in \mathbb{R}_+^* \times \mathbb{R} \\ & ((a, b) \cdot (c, d)) \cdot (e, f) = (ac, ad+b) \cdot (e, f) \\ & = (ace, ace + ad + b) \end{aligned}$$

$$\begin{aligned} & ((a, b) \cdot (c, d)) \cdot (e, f) = (a, b) \cdot (ce, cf+d) \\ & = (ace, acf + ad + b) \\ & = (a, b) \cdot (ce, cf+d) \\ & = ((a, b) \cdot (c, d)) \cdot (e, f). \end{aligned}$$

$$\text{On a dc } (a,b)(1,0) = (a,b)$$

De plus,

$$(1,0) \cdot (a,b) = (1 \cdot a, 1 \cdot b + 0) = (a,b)$$

Donc $(1,0)$ est bien un élément neutre.

\rightarrow Symétric:

soit $(a,b) \in \mathbb{R}_+^* \times \mathbb{R}$,

on cherche $(c,d) \in \mathbb{R}_+^* \times \mathbb{R}$ tq

$$(a,b) \cdot (c,d) = (1,0)$$

$$(ac, ad+b) = (1,0).$$

$$\begin{cases} ac = 1 \\ ad + b = 0 \end{cases} \Leftrightarrow \begin{cases} c = \frac{1}{a} \\ d = -\frac{b}{a} \end{cases}.$$

$$\text{Donc } (a,b) \cdot \left(\frac{1}{a}, -\frac{b}{a}\right) = (1,0).$$

$$\text{Df, } \left(\frac{1}{a}, -\frac{b}{a}\right) \cdot (a,b) = \left(\frac{1}{a} \cdot a, \frac{1}{a} \cdot b + \left(-\frac{b}{a}\right)\right) \\ = (1,0)$$

$$\text{Donc } (a,b)^{-1} = \left(\frac{1}{a}, -\frac{b}{a}\right).$$

al $\mathbb{R}_+^* \times \mathbb{R}$ muni de cette loi est bien un groupe d'élément neutre $(1,0)$.

Ex 2 Mg or tt est d'un groupe G est involutif (i.e.: $\forall g \in G, g^2 = 1$) alors G est commutatif.

$$\begin{aligned} \Leftrightarrow G \text{ est commutatif} &\Leftrightarrow \forall g, h \in G \Rightarrow gh = hg \\ &\Leftrightarrow \forall g, h \in G \Rightarrow ghg^{-1}h^{-1} = 1 \end{aligned}$$

Or puisque g & h st involutifs, $g^{-1}=g$ et $h^{-1}=h$

Dc $ghg^{-1}h^{-1} = (gh)(gh) = 1$ car gh est involutif

al G est bien commutatif.

Ex 3 Mg tt groupe de cardinal un nombre premier est cyclique.

indic : Th de Lagrange.

Th de Lagrange :

soit G un g de cardinal n , soit $H \subset G$ un

g alors le cardinal de H divise n .

et, pr $g \in G$, \exists l'ordre de g est $\{g^n, n \in \mathbb{Z}\}$,

alors l'ordre de g divise n .

Suite ex 3 Moi tt gpe de cardinal un
nbr premier est cycliq

soit G un gpe de cardinal p premier
alors $p \geq 2$ de on pt choisir $g \in G \setminus \{1\}$.

Le sous-groupe $\langle g \rangle$ engendré par g possède
un cardinal q divise celui de G (d'après le
Th de Lagrange).

Donc $|\langle g \rangle| = 1$ ou p .

Si $\langle g \rangle$ contient au moins 1 & g .

Donc $|\langle g \rangle| = p$, $\langle g \rangle = G$.

Donc G est monogène, de cardinal fini,
c'est de un gpe cycliq.

Ex 4 Moi si G est un gpe de cardinal
 ≤ 5 alors G est commutatif.

Qu'en est-il pour gpe de cardinal 6?

si $m = 2, 3$ ou 5: Alors comme m est premier,
un gpe de cardinal m est cyclique.

Donc $G \cong \mathbb{Z}/m\mathbb{Z}$, dc G est commutatif.

si $m = 1$: Alors un gpe de card 1 est $G = \{1\}$.
C'est bien un gpe commutatif.

si $m = 4$: soit G un gpe de cardinal 4, $g \in G$.
D'après le Th de Lagrange, l'ordre de g divise 4,
dc ordre(g) = 1, 2 ou 4.

\rightarrow si g est d'ordre 4: alors $1, g, g^2, g^3$ st éts $\neq b$,
dc $G = \{1, g, g^2, g^3\} \cong \mathbb{Z}/4\mathbb{Z}$ (car cycliq
& de card 4)

Preuve gpe cycliq est commutatif:

soit G cycliq, soit $g \in G$ q engendre G alors si $h, k \in G$
alors $\exists n, m \in \mathbb{N}$ tq $h = g^n$, $k = g^m$.
 $h \cdot k = g^m \cdot g^n = g^{m+n} = g^n \cdot g^m = kh$ dc le gpe est commutatif.

\rightarrow si G est cyclique, alors $G \cong \mathbb{Z}/m\mathbb{Z}$
isomorpho \hookrightarrow commutatif

→ si g est d'ordre 4: alors $1, g, g^2, g^3$ st
éts \neq de $G = \{1, g, g^2, g^3\} \cong \mathbb{Z}/4\mathbb{Z}$

Donc G est groupe commutatif.

→ si tous les éts st d'ordre 1 ou 2.

Alors $\forall g \in G, g^2 = 1$. Dès d'après
l'¹ en 2, G est commutatif.

cas R

si G est de cardinal ≤ 5 ,

L G est commutatif.

@ Groupe de cardinal de 6 éts st
d'ordre 1 ou 2.

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0), (0,\bar{1}), (\bar{1},0), (\bar{1},\bar{1}), (a,b) + (c,d) = (a+c, b+d)\}$$

Qu'en est-il pour groupe de cardinal 6?
Pr $n \geq 6$, σ n'est plus vrai.

$|S_3| = 6$ & S_3 n'est pas commutatif.

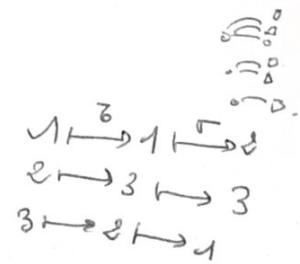
$$|S_3| = 3! = 6.$$

$$\tau = (1\ 2) \quad \text{et} \quad \sigma = (2\ 3)$$

$$\text{alors } \tau \circ \sigma = (1\ 2\ 3)$$

$$\text{De m } \sigma \circ \tau = (1\ 3\ 2).$$

Donc $\tau \sigma \neq \sigma \tau$, S_3 ne commute pas.



Exo Mg $(\mathbb{Q}, +)$ & (\mathbb{Q}_+^*, \times) ne
sont pas isomorphes. (indic : $\sqrt{2}$)

Supposons par l'absurde qu'il y ait
un isomorphisme.

$$\varphi: (\mathbb{Q}, +) \longrightarrow (\mathbb{Q}_+^*, \times)$$

alors φ est bijective &

$$\varphi(0) = 1$$

$$\varphi(a+b) = \varphi(a) \varphi(b)$$

$$\varphi(-a) = \frac{1}{\varphi(a)}$$

Idee : $\varrho \in \mathbb{Q}_+^*$, $\sqrt{2} \notin \mathbb{Q}_+^*$.

Comme φ est bijective, $\exists a \in \mathbb{Q}$ tq
 $\varphi(a) = \varrho$

Alors $(\varphi(\frac{a}{2}))^2 = \varphi(a) = \varrho$. | Donc les
groupes ne

Mais $\sqrt{2}$ n'est pas rationnel. | et pas
 $\varphi(\frac{a}{2})$ n'est pas défini. (c!c) | isomorphes.

(A)

Exo a) Mg groupe quotient \mathbb{R}/\mathbb{Z} est isomorphe
au groupe multiplicatif $S^1 = \{z \in \mathbb{C}, |z|=1\}$.

b) Mg groupe quotient \mathbb{C}/\mathbb{R} est isomorphe à \mathbb{R} .

Ex9 a) Montrer que le groupe quotient \mathbb{R}/\mathbb{Z} est isomorphe au groupe multip.

$$\mathbb{S}^1 = \{z \in \mathbb{C}, |z|=1\}$$

On va construire un isomorphisme

$$\varphi: \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{S}^1.$$

Pour cela il suffit trouver un morphisme

$\varphi: \mathbb{R} \rightarrow \mathbb{S}^1$ surjectif & tel que $\text{ker } \varphi = \mathbb{Z}$.

$$\varphi: t \mapsto e^{2i\pi t}$$

• Morphisme: soit $t, u \in \mathbb{R}$,

$$\begin{aligned}\varphi(t-u) &= e^{2i\pi(t-u)} \\ &= e^{2i\pi t - 2i\pi u} \\ &= e^{2i\pi t} \cdot (e^{-2i\pi u})^{-1}\end{aligned}$$

$$\varphi(t-u) = \varphi(t) \cdot \varphi(u)^{-1}$$

• Définir sur \mathbb{R}/\mathbb{Z} : si $\bar{t} = \bar{u}$ dans \mathbb{R}/\mathbb{Z} ,
ie si $t = u + k$ et $k \in \mathbb{Z}$ alors

$$\begin{aligned}\varphi(t) &= \varphi(u+k) = e^{2i\pi u} \cdot e^{2i\pi k} = \varphi(u). \\ \varphi(t) &= \varphi(u)\end{aligned}$$

On peut définir $\bar{\varphi}: \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{S}^1$

• $\bar{\varphi}$ est injectif

~~Si $\bar{t} = \bar{u}$ dans \mathbb{R}/\mathbb{Z} , ie si $t = u + k$, $k \in \mathbb{Z}$ alors $\varphi(t) = \varphi(u+k) = e^{2i\pi u} \cdot e^{2i\pi k} = \varphi(u)$~~

Supposons $\bar{\varphi}(t) = \bar{\varphi}(u)$, ie $\varphi(t) = \varphi(u)$,

$$e^{2i\pi t} = e^{2i\pi u} \Leftrightarrow e^{2i\pi(t-u)} = 1$$

de $t-u \in \mathbb{Z}$, ie $t=u$.

• $\bar{\varphi}$ est surjective (Il est de \mathbb{S}^1 possède bien un antécédent).

Soit $z \in \mathbb{S}^1$, pt écrire $z = e^{i\theta}$ on a $|z| = 1$ & de $z = e^{i\theta} = \varphi\left(\frac{\theta}{2\pi}\right) = \bar{\varphi}\left(\frac{\theta}{2\pi}\right)$

cl $\bar{\varphi}: \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{S}^1$ est isomorphisme de groupes.

Prop en + soit $\varphi: G \rightarrow H$ tq
 $\forall a, b: \varphi(a b^{-1}) = \varphi(a) \cdot \varphi(b)^{-1}$

Alors φ MDG.

Dm

- soit $a \in G, \varphi(1_G) = \varphi(a a^{-1})$
 $= \varphi(a) \varphi(a)^{-1} = 1$

- soit $a \in G, \varphi(a^{-1}) = \varphi(1_G \cdot a^{-1})$
 $= \varphi(1_G) \cdot \varphi(a)^{-1} = \varphi(a)^{-1}$

soit $a, b \in G,$

$$\varphi(ab) = \varphi(a(b^{-1})^{-1}) = \varphi(a) \varphi(b^{-1})^{-1} = \varphi(a) \varphi(b)$$

e) Mg le groupe quotient \mathbb{C}/\mathbb{R}
est isomorphe à \mathbb{R} .

M1 $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$

\downarrow quotient

$$\mathbb{C}/\mathbb{R} \cong (\mathbb{R} \times \mathbb{R})/\mathbb{R} \cong \mathbb{R}.$$

M2 $f_m: \mathbb{C} \rightarrow \mathbb{R}$

• Morphisme: $a+ib, c+id \in \mathbb{C}$, alors

$$\begin{aligned} f_m((a+ib) - (c+id)) &= f_m((a-c) + i(b-d)) \\ &= b-d = f_m(a+ib) - f_m(c+id) \end{aligned}$$

• $\text{Ker}(f_m) = \mathbb{R}$

$$f_m(z) = 0 \Leftrightarrow z \in \mathbb{R}.$$

Donc $f_m: \mathbb{C}/\mathbb{R} \rightarrow \mathbb{R}$ est defined & injective.

• Surjectif: soit $n \in \mathbb{R}$, $z \in f_m(\mathbb{R})$.

al On a bien un isomorphisme de groupes

$$f_m: \mathbb{C}/\mathbb{R} \rightarrow \mathbb{R}.$$

E14

Soit $H, K \subsetneq G$ deux \textcircled{g} de G .

a) Montrons que HUK est \textcircled{g} de G si $HCK = KCH$.

(\Leftarrow) si HCK alors $HUK = K$

si KCH alors $HUK = H$

Dès lors 2 cas, HUK est \textcircled{g} de G .

(\Rightarrow) Supposons $H \not\subset K$ et $K \not\subset H$

alors $\exists h \in H$ tq $h \notin K$.

$\exists k \in K$ tq $k \notin H$.

Montrons que $hk \notin HUK$

• si $hk \in H$, alors $h = h(hk)h^{-1} \in H$.

Contd $\textcircled{?}$

• si $hk \in K$, alors $h = (hk)k^{-1} \in K$.

Contd $\textcircled{?}$

Donc $hk \notin HUK$.

HUK n'est pas stable par la loi de G ,
ce n'est pas un \textcircled{g} de G .

Par contre posé, si HUK est un \textcircled{g} de G , alors $HCK = KCH$.

b) Si $A, B \subsetneq G$, on note

$$AB = \{ab \mid a \in A, b \in B\}.$$

Montrons que HK est \textcircled{g} de G si $HK = KH$.

(\Leftarrow) \triangleleft $HK = KH$ ne signifie pas que les éléments commutent.

Cela signifie si $hk \in HK \Rightarrow \exists h' \in H, k' \in K$ tq $hk = h'k'$.

Supposons $HK = KH$, soit $hk \in HK$, $h'k' \in HK$.

$$\text{alors } (hk)(h'k')^{-1} = \underbrace{hk}_{\in K} \underbrace{k'^{-1}h'^{-1}}_{\in H}$$

Donc $hk^{-1}h'^{-1} \in KH = HK$, $\exists h'' \in H$ de

$$h'' \in H, k'' \in K \text{ tq } hk^{-1}h'^{-1} = h''k''.$$

$$\text{Donc } (hk)(h'k')^{-1} = \underbrace{hh''}_{\in H} k'' \in HK$$

Donc HK est bien un \textcircled{g} de G .

\Leftrightarrow Suppos HK $\neq KH$,

alors soit $\exists hk \in HK$ tq $hk \notin KH$.
soit $\exists kh \in KH$ tq $kh \notin HK$.

Quitte à échanger les rôles de H & K,
Suppos qu'on est du b 2° cas.

On a $k = 1 \cdot k \in HK$
 $h = h \cdot 1 \in HK$.

Mais $hk \notin HK$.

De HK n'est pas un \textcircled{sg} de G.

Pour contraposée, si HK est un \textcircled{sg} de G,
alors $HK = KH$.

Ex 1)

soit $G \textcircled{sg}$, le centre $Z(G) = \{g \in G, gx = xg, \forall x \in G\}$

a) Mg $Z(G)$ est \textcircled{sg} distingué commutatif de G

b) Mg G est commutatif $\Leftrightarrow Z(G) = G \Leftrightarrow \%_{Z(G)}$ monog.

$\textcircled{*} \textcircled{sg}$ de G :

- $\forall n \in G, n \cdot 1 = 1 \cdot n = n$ dc $1 \in Z(G)$
- soit $g, h \in Z(G)$, alors $\forall n \in G$,
 $(gh)n = gnh = n(gh)$, dc $gh \in Z(G)$.

• soit $g \in Z(G)$ alors $\forall n \in G$,
 $(g^{-1}n)g = g^{-1}gn = n = (ng^{-1})g \Leftrightarrow g^{-1}n = ng^{-1}$
dc $g^{-1} \in Z(G)$.

Donc $Z(G)$ est bien un \textcircled{sg} de G.

$\textcircled{*} \textcircled{sg}$ distingué

soit $h \in Z(G), g \in G$, mg $ghg^{-1} \in Z(G)$
(alors $(ghg^{-1})x = ggg^{-1}hx = xhgg^{-1} = x(ghg^{-1})$)

De $ghg^{-1} \in Z(G)$ d'où $Z(G) \triangleleft G$
alors $ghg^{-1} = hgg^{-1} = h \in Z(G)$ dc $Z(G) \triangleleft G$

\textcircled{sg} commutativité :

soit $g, h \in Z(G)$, alors $gh = hg$
car $g \in Z(G)$.

Donc $Z(G)$ est commutatif

Groupe quotient

G un \textcircled{g} , $H \textcircled{sg}$

$G/H = \{gH, g \in G\} =$ classes d'équivalences pr
la relation $g Rh$ si $gh = hg$.

$H \setminus G = \{Hg, g \in G\}$: en général $H \setminus G \neq G/H$.

Supposons à présent que H est un \textcircled{sg} distingué de G . En effet, cela signifie que

$$hg \in H, \quad gHg^{-1} = H$$

$$\Leftrightarrow hg \in G, \quad gh = hg.$$

On a alors $H \setminus G = G/H$.

On peut munir alors G/H de la loi

$$gH \cdot g'H = (gg')H$$

$\rightarrow G/H$ est alors de groupe, de neutre $H = \textcircled{H=1}$.
& l'inverse de gH est $g^{-1}H$.

$$\text{où } gH = \{gh \text{ pr } h \in H\}$$

Pour simplifier les manipulations, on peut écrire :

$$G/H = \{\bar{g}, g \in G\},$$

où $\bar{g} = gH$ est la classe de g par la relation $gRh \Leftrightarrow gh^{-1} \in H$.

La f $G \rightarrow G/H$ est un MDG

$$g \mapsto gH$$

Q1. • $G = (\mathbb{Z}, +)$; $H = n\mathbb{Z}$ pr $n \in \mathbb{N}^*$.

$$H \triangleleft G, \quad G/H = \mathbb{Z}/n\mathbb{Z}.$$

• $G = GL_n(\mathbb{R})$, $H = SL_n(\mathbb{R})$

$$= \{A \in GL_n(\mathbb{R}), \det(A) = 1\}$$

$$SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$$

En effet, si $A \in SL_n(\mathbb{R})$, $P \in GL_n(\mathbb{R})$

$$\det(PAP^{-1}) = \det(P) \cdot \det(A) \cdot \det(P^{-1}) = 1$$

De $PAP^{-1} \in SL_n(\mathbb{R})$,

$SL_n(\mathbb{R})$ bien distingué.

soit $A, B \in GL_m(\mathbb{R})$

$$A SL_m(\mathbb{R}) = B SL_m(\mathbb{R}) \Leftrightarrow AB^{-1} \in SL_m(\mathbb{R})$$

$$\Leftrightarrow \det(AB^{-1}) = 1$$

$$\Leftrightarrow \det(A) \cdot \det(B)^{-1} = 1$$

$$\Leftrightarrow \det(A) = \det(B)$$

Donc $GL_m(\mathbb{R}) / SL_m(\mathbb{R})$ est l'ensemble de tous les déterminants, dc \mathbb{R}^* .

$\det : GL_m(\mathbb{R}) \rightarrow (\mathbb{R}^*)$ est un morphisme.

$\det : GL_m(\mathbb{R}) / SL_m(\mathbb{R}) \xrightarrow{\sim} (\mathbb{R}^*)$ est un isomorphisme

$$\text{tq } \ker(\det) = SL_m(\mathbb{R})$$

* Injectif: soit $x \in \mathbb{R}^*$, $x = \det \begin{pmatrix} * & * \\ * & * \\ \vdots & \vdots \\ 0 & 1 \end{pmatrix}$ $\Leftrightarrow G/Z(G)$ est monog.

* injectif: soit A tq $\det(A) = 1$.

$$\text{tq } A \in SL_m(\mathbb{R})$$

$$\bar{A} = A SL_m(\mathbb{R}) = SL_m(\mathbb{R})$$

$$\bar{A} = 1_{GL_m(\mathbb{R}) / SL_m(\mathbb{R})}$$

Donc $\ker(\det) = \{1_{GL_m(\mathbb{R}) / SL_m(\mathbb{R})}\}$

mq MDG est injectif, il suffit de mq le moyen est égal à 1.

Ex (f) Mg ASSE

G est commutatif $\Leftrightarrow Z(G) = G \Leftrightarrow G/Z(G)$ est monog.

(i) \Rightarrow (ii):

$Z(G) = \{g \in G, gn = ng, \forall n \in \mathbb{Z}\} = G$
car comme G est commutatif, tt est vérifié cela

(ii) \Rightarrow (iii) supposons $Z(G) = G$,

$$\text{alors } G/Z(G) = G/G = \{gG, g \in G\} = \{G\}$$

$$\text{d'où } G/Z(G) \cong \{1\}.$$

(iii) \Rightarrow (i) sps $G/Z(G) = \langle \bar{g} \rangle = \langle gZ(G) \rangle$

cela signifie que si $\bar{g} \in G$ alors $\exists m \in \mathbb{Z}$ tq $\bar{g} \in gZ(G) = g^m Z(G)$

(iii) \Rightarrow (i) opps $\mathbb{Z}(G) = \langle \bar{g} \rangle = \langle g \mathbb{Z}(G) \rangle$

ce qui signifie que si $g' \in G$

alors $\exists m \in \mathbb{Z}$ tq $g' \mathbb{Z}(G) = g^m \mathbb{Z}(G)$

i.e., tt elt $g' \in G$ s'écrit

$$g' = g^m h \quad \forall m \in \mathbb{Z}, h \in \mathbb{Z}(G)$$

soit $g', g'' \in G$,

$$\text{on écrit } g' = g^m h \quad \text{et } m, n \in \mathbb{Z} \\ g'' = g^n k \quad h, k \in \mathbb{Z}(G)$$

$$\text{Alors } g'g'' = g^m h g^n k = g^m g^n h k = g^m g^n k h \\ = g^{m+n} h k \Rightarrow g'g'' = g''g'$$

Donc G est commutatif.

Ex 18 Groupe dérivé

soit G un \mathbb{G} , le groupe dérivé de G est le $\mathbb{D}(G)$ de G engendré par les commutateurs :

$$\mathbb{D}(G) = \langle ghg^{-1}h^{-1} \mid g, h \in G \rangle$$

Mq $\mathbb{D}(G)$ est le plus petit \mathbb{G} distingué de G pour lequel le \mathbb{G} quotient $G/\mathbb{D}(G)$ est commutatif.

$\mathbb{D}(G)$ \mathbb{G} distingué ?

soit $c = ghg^{-1}h^{-1}$ un commutateur,

$$\text{soit } a \in G, \text{ alors } acca^{-1} = agh g^{-1} h^{-1} a^{-1} \\ = [(ag)h(a g)^{-1} h^{-1}] [h a h^{-1} a^{-1}] \in \mathbb{D}(G)$$

comme $(ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1}$, tout elt de $\mathbb{D}(G)$ se écrit $c_1 \dots c_n$ + c_i des commutateurs.

$$\text{si } a \in G, \text{ on a } a(c_1 \dots c_n)a^{-1} = \\ (a \cdot c_1 a^{-1}) \dots (a c_n a^{-1}) \in \mathbb{D}(G).$$

Donc $aD(G)a^{-1} \subset D(G) \quad \forall a \in G.$

D'où $D(G) \triangleleft G.$

• $G/D(G)$ est commutatif

soit $g, h \in G.$

On a $ghg^{-1}h^{-1} \in D(G)$

Donc dans $G/D(G), \quad ghg^{-1}h^{-1} = \overset{G/D(G)}{=} 1 = ghg^{-1}h^{-1}D(G) = D(G)$

$$ghg^{-1}h^{-1} = 1 = ghg^{-1}h^{-1}$$

$$\bar{g}\bar{h} = \bar{h}\bar{g}$$

Donc $G/D(G)$ est commutatif.

• $D(G)$ minimal par cette prop'

soit $H \triangleleft G$ tq G/H est commutatif.

soit $\bar{g}, \bar{h} \in G$, alors ds G/H ,

$$\bar{g}\bar{h}\bar{g}^{-1}\bar{h}^{-1} = 1$$

de $ghg^{-1}h^{-1} \in H.$

H contient tous les commutateurs.

Donc H contient $D(G).$

$D(G)$ est bien le + petit $\textcircled{2}$ distingué de G tq $G/D(G)$ commute.

(+ petit : il est contenu de n'importe quel $\textcircled{2}$)

Exercice soit $G \textcircled{2}$, $\forall g \in G$, $\varphi_g: G \rightarrow G$

a) Vérifier φ_g est automorphisme de G . $x \mapsto gxg^{-1}$ pour \forall

b) Vérifier que $\text{Aut}(G)$ des automorphismes de G est un groupe (par la loi de composition).

c) Montrer l'appli $\Psi: G \rightarrow \text{Aut}(G)$, $g \mapsto \varphi_g$ est un MDB

d) Déterminer le no de Ψ

e) Montrer l'image de Ψ est $\textcircled{2}$ distingué de $\text{Aut}(G)$.

Résultat Exo $g \in G$, $\psi_g : G \rightarrow G$,

$$\psi_g(x) = g x g^{-1} \quad \forall x \in G.$$

a) Vérifions ψ_g est automorphisme de G .

$$\begin{aligned}\psi_g : G &\longrightarrow G \\ x &\longmapsto g x g^{-1}\end{aligned}$$

ψ_g est un morphisme $\forall x, y \in G$.

$$\begin{aligned}\psi_g(xy) &= g(x y^{-1}) g^{-1} = g x g^{-1} g y g^{-1} \\ &= (g x g^{-1}) g y g^{-1}\end{aligned}$$

$$\psi_g(xy) = \psi_g(x) \cdot \psi_g(y)$$

ψ_g est une bijection

$$\begin{aligned}\psi_g(x) = y &\Leftrightarrow g x g^{-1} = y \\ &\Leftrightarrow x = g^{-1} y g \\ &\Leftrightarrow x = \psi_{g^{-1}}(y)\end{aligned}$$

ψ_g est bien bijective et l'inverse ψ_g^{-1} .

Donc $\psi_g : G \rightarrow G$ est bien automorphisme. (26)

b) Vérifier $\text{Aut}(G)$ est un (g).

$\text{Aut}(G)$ est associatif.

$a, b, c \in \text{Aut}(G), x \in G$,

$$\begin{aligned}(a \circ b) \circ c(x) &= (a \circ b)(c(x)) = a(b(c(x))) \\ &= a(b \circ c(x)) = a \circ (b \circ c)(x)\end{aligned}$$

Donc $(a \circ b) \circ c = a \circ (b \circ c)$.

$\text{Aut}(G)$ est stable par composition

si $\varphi, \psi \in \text{Aut}(G)$; $\varphi \circ \psi$ est toujours bijective
& $\forall x, y \in G$,

$$(\varphi \circ \psi)(xy) = \varphi(\psi(x)\psi(y)) = (\varphi \circ \psi)(x)(\varphi \circ \psi)(y)$$

Donc $\varphi \circ \psi$ est encore un automorphisme

Neutre

On cherche un neutre $\varepsilon \in \text{Aut}(G)$ alors

$$\forall \varphi \in \text{Aut}(G), \varepsilon \circ \varphi = \varphi \circ \varepsilon = \varphi \text{ i.e. } \forall x \in G$$
$$\varepsilon(\varphi(x)) = \varphi(\varepsilon(x)) = \varphi(x)$$

Possible si $\varepsilon = \text{Id}_G$. Donc Id_G est le neutre de $\text{Aut}(G)$.

Inverse soit $\varphi \in \text{Aut}(G)$,

de φ possède une réciproque $\varphi^{-1}: G \rightarrow G$

$$\text{tq } \varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \text{Id}_G$$

φ^{-1} est-il un automorphisme ?

On sait déjà que c'est une bijection.

$$\begin{aligned} \varphi \circ \varphi^{-1}(xy) &= xy = (\varphi \circ \varphi^{-1})(x)(\varphi \circ \varphi^{-1})(y) \\ \varphi^{-1}(xy) &= \varphi^{-1}(x) \varphi^{-1}(y) \end{aligned}$$

Donc φ^{-1} est bien un morphisme, de plus un automorphisme,

$\Rightarrow (\text{Aut}(G), \circ)$ est bien un g.

$$\begin{aligned} * &= \varphi(\varphi^{-1}(x) \varphi^{-1}(y)) \quad \downarrow \varphi \text{ injectif} \\ \varphi^{-1}(xy) &= \varphi^{-1}(x) \varphi^{-1}(y). \end{aligned}$$

c) Mq $\varphi: G \rightarrow \text{Aut}(G)$ et M.D.G

soit $g, h \in G$, on a $\varphi(gh) = \varphi(g)\varphi(h)$

soit $x \in G$,

$$\begin{aligned} \varphi_{gh}(x) &= (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = g(hxh^{-1})g^{-1} \\ &= \varphi_g \circ \varphi_h(x) \end{aligned}$$

M.D.G $G \rightarrow \text{Aut}(G)$

d) Déterminer le noyau de φ .

$$\text{ker } \varphi = \{g \in G, \varphi_g = \text{Id}_G\}$$

$$= \{g \in G, \forall x \in G, gxg^{-1} = x\}$$

$$= \{g \in G, \forall x \in G, gx = xg\} = Z(G)$$

e) Mq l'image de φ est g distingué de $\text{Aut}(G)$.

soit $\varphi_g \in \text{Im } \varphi$, soit $\varphi \in \text{Aut}(G)$,

$$\text{alors } \forall x \in G, \varphi \circ \varphi_g \circ \varphi^{-1}(x) = (\varphi \circ \varphi_g)(\varphi^{-1}(x))$$

$$= \varphi(g \varphi^{-1}(x) g^{-1}) = \varphi_g \varphi \varphi^{-1}(x) \varphi(g^{-1})$$

$$= \varphi(g) x (\varphi(g))^{-1} = \varphi_{\varphi(g)}(x) \in \text{Im } \varphi$$

27 $\Rightarrow \text{Im } \varphi \subset \text{Aut}(G)$

Actions de Groupes

- Une **action** de groupe G sur l'ens A , c'est une application $G \times A \rightarrow A$

$$(g, a) \mapsto g \cdot a$$

Vérifiant:

$$\textcircled{1} \quad \forall a \in A, 1_G \cdot a = a$$

$$\textcircled{2} \quad \forall g, h \in G, \forall a \in A, g \cdot (h \cdot a) = (gh) \cdot a$$

- RQ** Une action de groupe, c'est la donnée d'un morphisme $\theta : G \rightarrow S(A)$ permutations des élts de A .



1. e Le stabilisateur d'un élé de A , c'est

$$\text{Stab}_a = \{g \in G, g \cdot a = a\}$$

Stab_a est un **sg** de G .

Ex 29 Déterminer les orbites de l'action de $GL_n(\mathbb{R})$ sur \mathbb{R}^n .

L'action de $GL_n(\mathbb{R})$ sur \mathbb{R}^n . Prendre $A \cdot x = g(x)$ où $g \in GL_n(\mathbb{R})$ est l'isomorphisme associé à A de la base canonique voir les élts de \mathbb{R}^n à des matrices colonnes $1 \times n$ telles que $A \cdot X = AX$.

$$GL_n(\mathbb{R}) \curvearrowright \mathbb{R}^n \text{ (opér.)}$$

On va voir \mathbb{R}^n l'ens des vect^{RS} colonnes $\mathbb{C}^{1 \times n}(\mathbb{R})$ L'action est $A \cdot x = AX$.

Vérifions c'est bien une act de groupe.

$$1) \text{ soit } x \in \mathbb{R}^n, I_n \cdot x = x$$

$$2) \text{ soit } A, B \in GL_n(\mathbb{R}), x \in \mathbb{R}^n$$

$$A \cdot (B \cdot x) = A \cdot (BX) = ABX = (AB) \cdot x.$$

soit $X \in \mathbb{R}^n$, l'orbite de X est $\mathcal{O}_X = \{A \cdot X \text{ pour } A \in GL_n(\mathbb{R})\}$.
 Soit $y \in \mathbb{R}^n \setminus \{0\}$. Donc $n \neq 0$, $\mathcal{O}_y = \mathbb{R}^n \setminus \{0\}$.

On cherche de déterminer à X fixé tous les $Y \in \mathbb{R}^n$ qui peuvent être obtenus par multiplication de X par une matrice de $GL_n(\mathbb{R})$.

Il faudra faire une distinction de cas entre le cas où $X=0$ & le cas où $X \in \mathbb{R}^n \setminus \{0\}$.

cas $X=0$:

Pour la matrice $g \in GL_n(\mathbb{R})$, $g \cdot 0 = g(0) = 0$.

Donc $\mathcal{O}_0 = \{0\}$.

en $X \in \mathbb{R}^n \setminus \{0\}$:

soit $y \in \mathbb{R}^n \setminus \{0\}$,

→ soit B_1 une base de \mathbb{R}^n dont le 1^{er} vecteur est x .

→ soit B_2 une base de \mathbb{R}^n dont le 1^{er} vecteur est y .

→ soit $g \in GL_n(\mathbb{R})$ la mat de passage de B_1 à B_2 .
 Alors $g \cdot x = y$.

Donc $n \neq 0$, $\mathcal{O}_x = \mathbb{R}^n \setminus \{0\}$.

Ex 30

Vérifier \mathbb{R} agit sur \mathbb{C} par $(\theta, z) \in \mathbb{R} \times \mathbb{C}$

→ $\theta \cdot z = e^{i\theta} z$. Décrire les orbites de cette action.

$\mathbb{R} \curvearrowright \mathbb{C}$, $\theta \cdot z = e^{i\theta} z$, soit $z \in \mathbb{C}$ alors $\forall \theta \in \mathbb{R}$

$$|\theta \cdot z| = |e^{i\theta} z| = |e^{i\theta}| \cdot |z| = |z|$$

Réciproquement, si $|z| = |z'| \neq 0$ alors $|\frac{z'}{z}| = \frac{|z'|}{|z|} = 1$

de $\exists \theta \in \mathbb{R}$ tq $\frac{z'}{z} = e^{i\theta}$ i.e. $z' = z \cdot e^{i\theta} = \theta \cdot z$.

Rés: $\mathcal{O}_z = S^1(0, z)$.

Les orbites sont les cercles de centre 0.

Prop^m Soit $G \curvearrowright X$, $\forall x \in X$,
On est un bijo $\varphi: G/\text{Stab}(x) \rightarrow \Omega_x$.

FH (Équations formules aux classes).

Soit $G \curvearrowright X$, X fini.

Soit x_1, \dots, x_n des représentants des orbites

alors $|X| = \sum_{i=1}^n [G : \text{Stab}(x_i)] = \frac{|G|}{|\text{Stab}(x_i)|}$

Démonstration $|X| = \sum_{i=1}^n |\Omega_{x_i}| = \sum_{i=1}^n |G/\text{Stab}(x_i)|$
 $= \sum_{i=1}^n [G : \text{Stab}(x_i)]$

Ex 33 FF de Burnside

Soit G fini agissant sur un X fini. Pq $g \in G$,
on note $\chi(g)$ le nbr de pts de X fixés par g .

Mq

(N) $N = \frac{1}{|G|} \sum_{g \in G} (\chi(g))$ — nbr pts X fixés par g

nbr orbites
de l'act.

On dénombre $S = \{(g, x) \in G \times X, g \cdot x = x\}$.
de 2 manières différentes.

M.1 $S = \bigcup_{g \in G} \{(g, x), \exists x \in X \text{ tq } g \cdot x = x\}$.

$|S| = \sum_{g \in G} |X(g)|$

M.2 $S = \bigcup_{x \in X} \{(g, x) \text{ tq } g \in G \text{ et } g \cdot x = x\}$.

$S = \bigcup_{x \in X} \{(g, x) \text{ tq } g \in \text{Stab}(x)\}$.

$|S| = \sum_{x \in X} |\text{Stab}(x)|$

Soit x_1, \dots, x_N des représentants des orbites.

$$\begin{aligned} |S| &= \sum_{i=1}^N \sum_{x \in \Omega_{x_i}} |\text{Stab}(x_i)| \\ &= \sum_{i=1}^N |\Omega_{x_i}| \times |\text{Stab}(x_i)| \\ &= \sum_{i=1}^N \frac{|G|}{|\text{Stab}(x_i)|} \times |\text{Stab}(x_i)| = N \cdot |G| = |S| \end{aligned}$$

30

$$\text{cd} \quad N \times |G| = \sum_{g \in G} \chi(g)$$

$$\Rightarrow \boxed{N = \frac{1}{|G|} \sum_{g \in G} \chi(g)}$$



Bonus

On a des perles de 3 couleurs différentes.
Combien de bracelets différents pourront faire de 5 perles?

$$clR = \{ R, V, B \}$$

Appelé Bernoulli.


Rotat.

$$\begin{matrix} R & R \\ R & B \end{matrix} \vee = \begin{matrix} R & B \\ B & R \end{matrix} \vee$$

Ex 35 (Normalisateur d'un \$\mathfrak{H}\$)

soit \$G\$ \$\mathfrak{G}\$, \$H\$ \$\mathfrak{H}\$ de \$G\$. Le normalisateur de \$H\$ de \$G\$ est

$$N_G(H) = \{g \in G \mid g H g^{-1} = H\}$$

a) Montrer que \$N_G(H)\$ est le plus petit \$\mathfrak{G}\$ de \$G\$ contenant \$H\$ et \$\mathfrak{g}\$ distingué.

b) Montrer que le nombre \$\mathfrak{G}\$ distincts conjugués de \$H\$ de \$G\$ est égal \$[G : N_G(H)]\$

$$a) N_G(H) = \{g \in G, g H g^{-1} = H\}$$

Montrer c'est \$\mathfrak{G}\$

$$\text{neutre} \quad 1 H 1^{-1} = H \quad \text{de } 1 \in N_G(H).$$

$$\text{inverse} \quad g \in N_G(H), \quad g^{-1} H g = g^{-1} (g H g^{-1}) g = H \quad \text{de } g^{-1} \in N_G(H)$$

$$\text{stabilité} \quad g, h \in N_G(H), \quad (gh) H (gh)^{-1} = gh H h^{-1} g^{-1} = g H g^{-1} = H, \\ g h \in N_G(H).$$

Donc \$N_G(H)\$ est \$\mathfrak{G}\$ de \$G\$.

soit \$h \in H\$, \$h H h^{-1} = H\$ de \$h \in N_G(H)\$, \$H \subset N_G(H)

soit \$g \in N_G(H)\$, \$g H g^{-1} = H\$ par définition, d'où \$H \subset N_G(H)\$.

(31)

le + grad :

soit $K \triangleleft G$ contenant H & tq $H \triangleleft K$.

si $g \in K$, $\hat{e} H$ est distingué de K ,

$$gHg^{-1} = H.$$

De $K \subset N_G(H)$.

$N_G(H)$ est de bien le + grad (sg) .

b) $\#$ mbr (sg) distincts conjugués de H ds G est égal à $[G : N_G(H)]$.

On \oplus l'act suivante de G sur les (sg) de G def par $g \cdot K = gKg^{-1}$

Alors \mathcal{Q}_H est l'ensemble des (sg) conjugués à H .

$N_G(H) = \text{Stab}(H)$. $\triangle \triangle^{\text{voir}}$

Donc \mathcal{Q}_H est en bijection de $G/\text{Stab}(H)$.

ie l'ensemble des (sg) de G conjugués à H est en biject w/ $G/N_G(H)$. (32)

Le nbr de (sg) de G conjugués à H est dc $|G/N_G(H)| = [G : N_G(H)]$.

$$\{gHg^{-1}, g \in G\}; N_G(H) = \{g \in G, gHg^{-1} = H\}.$$

Ex 36 Th de Cayley.

Mq Φ s'injecte ds le $\text{Bij}(G)$

indic: faire agir G sur lui-m^{me} p translat à gauche

Comme toute action, elle définit un morphisme: $\Pi: G \rightarrow \text{Bij}(G)$

$$g \mapsto \Pi_g$$

$$\text{où } \Pi_g(n) = g \cdot n = gn.$$

soit $g \in \ker \Phi$ alors $\Phi_g = \text{Id}_G$

$$\Phi_g(1) = 1$$

$$g \cdot 1 = 1$$

$$g = 1$$

Donc $\ker \Phi = \{1\}$, Φ est bien une inj ecut $G \hookrightarrow \text{Bij}(G)$.