<u>Lemme 1.2.7</u> : Supposons E fini, $\neq \emptyset$, dc il existe $a \in E$. Alors : $E \setminus \{a\}$ est fini et $\# E \setminus \{a\} = \# E - 1$.

<u>Dém</u> : On pose $n = \# E$, $\varphi : [\![1, n]\!] \xrightarrow{\sim} E$

- si $\varphi(n) = a$: on est content.
- sinon : transposition : $\tau : [\![1, n]\!] \xrightarrow{\sim} [\![1, n]\!]$ qui échange n et p, où $p = \varphi^{-1}(a)$

on pose : $\psi = \varphi \circ \tau$, dc : $\psi(n) = \varphi(\tau(n))$
$= \varphi(p) = a$

ds ts les cas : il existe $\psi : [\![1, n]\!] \xrightarrow{\sim} E$

tq. $\varphi(n) = a$.

Il est facile de mq $\varphi|_{[\![1, n-1]\!]} \longrightarrow E\setminus\{a\}$

est 1 bijection.

dc par déf : $E\setminus\{a\} \simeq [\![1, n-1]\!]$

dc $\# E\setminus\{a\} = n-1$.

$\square$

Th. 1.0.6 : Soit E fini et $F \subset E$.

Alors F est aussi fini, et $\# F \leq \# E$.

De plus : $(F \subset E \text{ et } \# F = \# E) \Leftrightarrow (F = E)$

Démo : Par réc, $\forall n \in \mathbb{N}$ posons :

(P_n) : Si E est fini de cardinal n, alors :

$\forall F \subset E$, F est fini, $\#F \leq n$

et si $\#F = n$, alors $F = E$.

- Si $\#E = 0$, alors $E = \emptyset$. Donc si $F \subset E$, $F = \emptyset$

donc : F est fini, $\#F = 0 \leq \#E = 0$, $\#F = \#E$ et $F = E$

donc (P_0) est vraie.

- Soit $n \in \mathbb{N}$ tq. (P_n) est vraie. Soit E fini de cardinal $(n+1)$. Soit $F \subset E$.

1er cas : si $F = E$: F est évidemment fini,
$\#F = \#E$

<u>2ème cas</u> : $F \subsetneq E$, il existe $a \in E \setminus F$.

donc : $F \subset E \setminus \{a\}$. Avec le lemme :

$\# E \setminus \{a\} = \# E - 1 = n$.

par hyp de réc : F est fini et $\# F \leq n$
$< n+1$
$< \# E$

On a mq : dans tous les cas, si $F \subset E$, F est fini et
$\# F \leq \# E$

Mais on a aussi mq :
$$\begin{cases} F = E \Rightarrow \# F = \# E & (1) \\ F \neq E \Rightarrow \# F < \# E & (2) \\ \qquad\qquad\quad \neq \# E & \end{cases}$$

(1) $\Rightarrow$ (2) $\Leftarrow$ par contraposition.

donc : $F = E \iff \# F = \# E$.

donc (P_{n+1}) est vraie. $\square$

Rq : pr mq. 2 ens E et F st égaux, on peut :

(1) $\forall x$, $x \in E \iff \dots \iff x \in F$

(2) dble inclusion.

nlle méthode : $\boxed{\text{(3) Si } E \text{ est fini}}$: mq. $F \subset E$ et $\# F = \# E$.

Th : Soit E et F 2 ensembles (qconques).

et $f : E \to F$.

(i) Si F est fini et f est injective, alors :

E est fini, et $\# E \leq \# F$

(ii) Si E est fini et f est surjective, alors :

F est fini, et $\# F \leq \# E$

(iii) Si F et E sont finis et $\# E = \# F$, alors :

f est injective $\iff$ f est surjective $\iff$ f est bijective.

Démo : (i) Rappel : $f|^{f(E)} : E \to f(E)$ est surjective.

dc si f est injective, $f|^{f(E)}$ est toujours injective,

dc elle est bijective : E et $f(E)$ sont équipotents,

or comme F est fini et $f(E) \subset F$, alors

$f(E)$ est fini aussi. Comme $f(E)$ est en

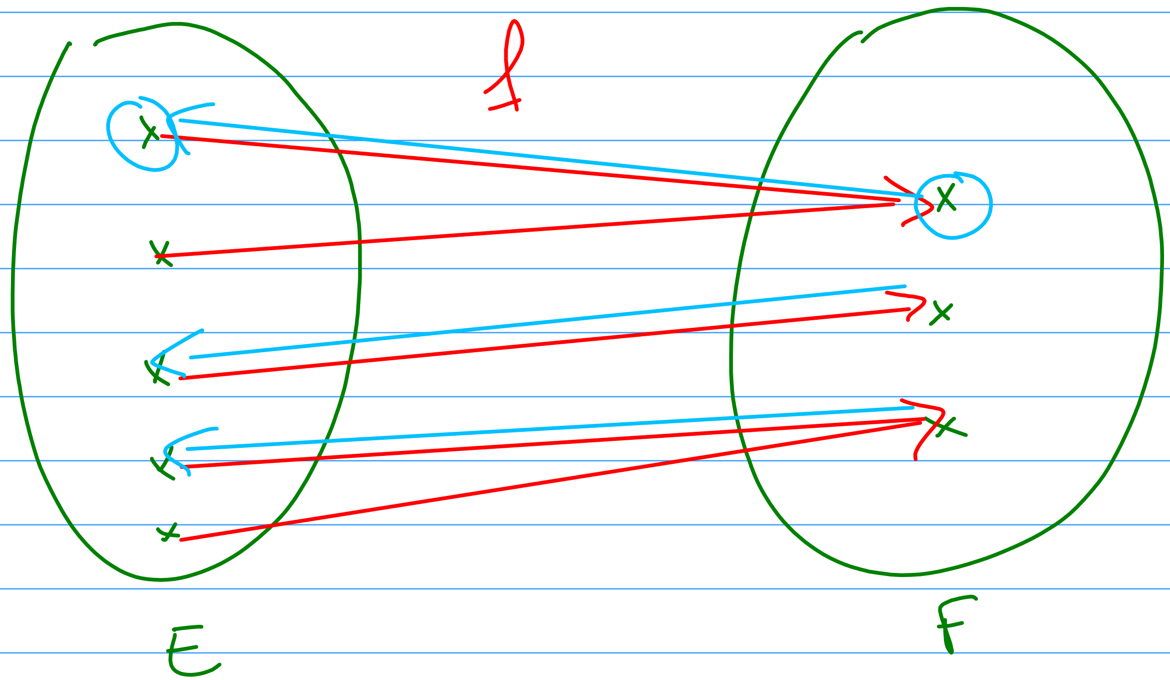
bijection avec E, E est fini et $\# E = \# f(E)$

$\leq \# F$ car $f(E) \subset F$

(ii) il repose sur 1 point plus délicat :

lemme 1.0.8 [si $f : E \to F$ est surjective, il existe 1 injection de $F \to E$.

démo du lemme 1.0.8 :



Soit $y \in F$. Puisque f est surjective, y a au moins 1 antécédent par f. Choisissons-en 1, on le note $g(y)$

En faisant cela $\forall y \in F$, nous avons construit 1 applica° $g : F \to E$. Montrons que cette applica° est injective. Soit $y_1, y_2 \in F$ tq. $g(y_1) = g(y_2)$.

Par construc°, $g(y_1)$ est 1 antécédent de y_1 par f,

dc : $f(g(y_1)) = y_1$.

De $\hat{m}$: $f(g(y_2)) = y_2$.

On a : $f \circ g = id_F$

dc $f \circ g$ est injec

$\Downarrow$

dc g injec.

dc : $g(y_1) = g(y_2) \Rightarrow f(g(y_1)) = f(g(y_2))$

$\Rightarrow y_1 = y_2$

dc g est injective. $\square$

En appliquant directe^t ce lemme lorsque $f : G \to F$ est surjective, il existe 1 injection $g : F \to E$,

dc si E est fini, avec (i), F est fini aussi

et $\# F \leq \# E$.

(iii) Soit $f : E \to F$ avec $\# E = \# F$.

- Si f est injective, f est 1 bijection de E ds $f(E)$

(c'est le m argument que ds la démo de (i))

dc : $\# E = \# f(E)$

mais $f(E) \subset F$

et $\# F = \# E = \# f(E)$

donc : $\begin{cases} f(E) \subset F \\ \# f(E) = \# F \end{cases}$, dc $f(E) = F$

dc f est surjective

dc : f injective $\Longrightarrow$ f surjective

- réciproque : supposons f surjective, mq. elle est injective.

Soit $x, y \in E$ tq. $f(x) = f(y)$.

Supposons que $x \neq y$, cherchons 1 contradiction.

$E' = E \setminus \{x\}$,

Soit $\tilde{f} : \begin{array}{l} E' \longrightarrow F \\ x \longmapsto f(x) \end{array}$ Mq. $\tilde{f}$ est surjective.

alors : Soit $z \in F$. Si $z \neq f(x)$, alors z a 1 antécédent par f (car f est surjective) et cet antécédent n'est pas x car $z \neq f(x)$.

Dc z a 1 antécédent ds E' : il a 1 antécédent par $\tilde{f}$

• si $z = f(x)$, dc ce cas $z = f(y)$

et $y \neq x$ dc $y \in E \setminus \{x\}$, $y \in E'$

z a 1 antécédent ds E', dc z a 1 antécédent par $\tilde{f}$.

On a mq. $\tilde{f}$ est surjec, dc avec (ii) : $\# E' \geq \# F$

or $\# E' = n-1$; $\# F = n$: ABSURDE.

dc f surjective $\Longrightarrow$ f injective.

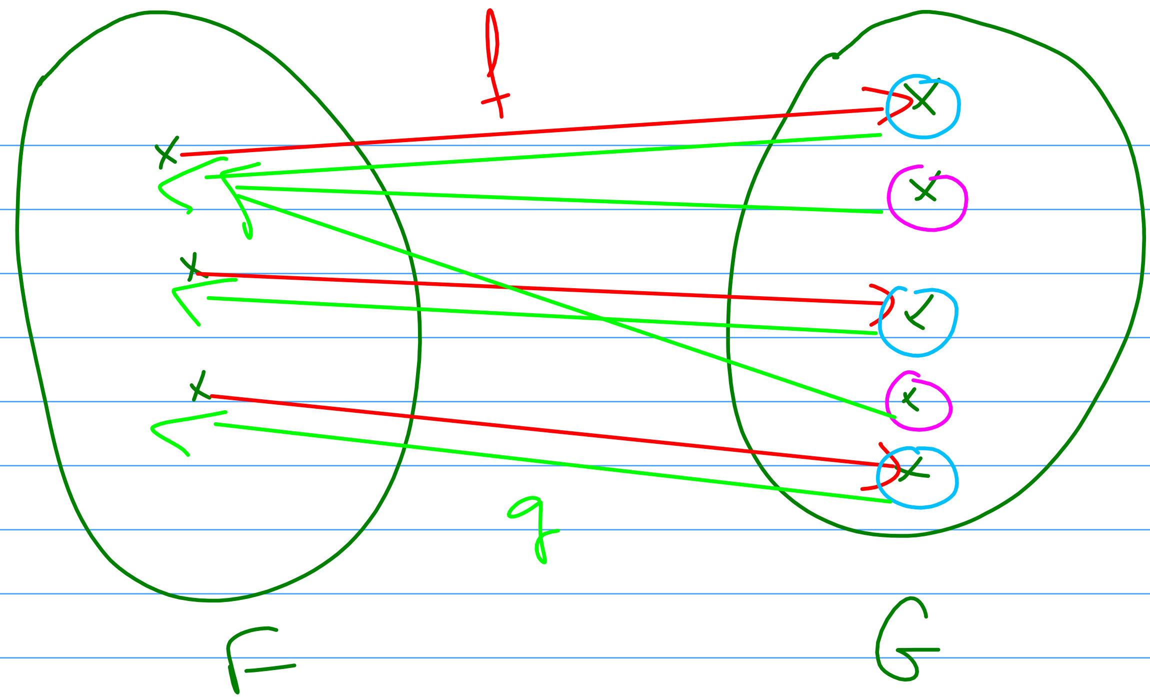
$$\begin{tikzcd}
 & f \text{ surjec.} \arrow[dl, Rightarrow, shift left] \arrow[dr, Rightarrow, shift left] & \\
f \text{ injec.} \arrow[ur, Rightarrow, shift left] & & f \text{ bijec} \arrow[ul, Rightarrow, shift left] \arrow[ll, Rightarrow]
\end{tikzcd}$$

f surjec

$\Longrightarrow$ f injec et surjec.

$\Longrightarrow$ f bijec.

Ex. 1.a.g :



Cor : principe des tiroirs : si $m, n \in \mathbb{N}$ t.q. $m < n$, il n'existe pas d'injection d'1 ens. de cardinal n dans un ensemble de cardinal m.

Dém : c'est la contraposée de (i).

1.2.13 : $(G, \star)$ 1 groupe, $A \subset G$

A finie, $A \neq \emptyset$, stable par $\star$ ($\forall x, y \in A$, $x \star y \in A$).

Mq. A est un sous-groupe de G.

il reste à mq : $\forall x \in A$, $x^{-1} \in A$.

Soit $x \in A$.

1) $\varphi : \mathbb{N}^* \longrightarrow G$ $\quad$ $(x^n = \underbrace{x \star x \star \cdots \star x}_{n \text{ fois}})$.

$n \longmapsto x^n$

$x \in A$ et A est stable par $\star$, dc : $x \star x \in A$

dc $x \star (x \star x) \in A$

par récurrence : $\forall n \in \mathbb{N}^*$, $x^n \in A$.

dc $\varphi : \mathbb{N}^* \longrightarrow A$. Or A est fini, dc

avec (i) [principe des tiroirs], si φ est injective,

$\mathbb{N}^*$ est fini (et $\# \mathbb{N}^* \leq \# A$)

ABSURDE, dc φ n'est pas injective.

2) Conclure : il existe $n, m \in \mathbb{N}^*$ tq. $\varphi(n) = \varphi(m)$

ie : $x^n = x^m$

traitons par ex le cas où $n < m$.

x est inversible ds G, dc $x^{m-n} = 1$ (1 : neutre de G)

Or $m - n \in \mathbb{N}^*$, dc $m - n \geq 1$

dc $x^{m-n-1} \times x = 1$ $(*)$

dc : x a pour inverse x^{m-n-1}.

. si $m-n-1=0$, alors $x^{m-n-1} = 1$ donc d'après la relation $(*)$: $x = 1$, donc $1 \in A$ et $x^{-1} = 1 \in A$

. si $m-n-1 > 0$: alors $x^{m-n-1} = \varphi(m-n-1) \in A$

donc $x^{-1} \in A$

Dans tous les cas, $x^{-1} \in A$ donc A est un sous-groupe de G.

<u>Ex. 1.0.17</u> : il y a 1 nb. d'états pour le cube.

On fixe 1 manipulation m.

On note M l'état du cube après avoir effectué m, et M^n son état après avoir effectué n fois la manip.

(On part du cube résolu).

$\varphi : \mathbb{N} \longrightarrow$ ensemble de ts les états du cube $) = E$

$n \longmapsto M^n$

hyp de départ : $\varphi(0) = M^0$ = cube résolu.

$\mathbb{N}$ est ∞, E est fini (qu : $\# E$?)

donner 1 majorant de $\# E$

dc φ n'est pas injective.

Mq. il existe $n \in \mathbb{N}^*$ tq. $\varphi(n)$ = cube résolu.

2) <u>Dénombrement :</u>

<u>Déf. 2.1.1 :</u> $A \sqcup B = A \amalg B$

$= (A \cup B$ avec l'indication que $A \cap B = \emptyset)$

$A \cup B$ se note $A \cup B$ si A et B ne sont pas disjoints

$A \cup B$ se note $A \sqcup B$ si A et B sont disjoints.

<u>notation officielle</u>.

<u>P. 2.1.2 :</u> Soit E 1 ens. fini et A et B 2 parties de E.

Donc A et B sont finies, et :

1) si $A \cap B = \emptyset$, $A \sqcup B$ est fini et $\# A \sqcup B = \# A + \# B$

3) cas g^{al} : $A\cup B$ est fini et $\# A\cup B = \# A + \# B - \# A\cap B$

2) $\# A\setminus B = \# A - \# A\cap B$

4) $\#(\complement_E A) = \# E - \# A$

Dém : seul le pt 1) est casse-pied.

les 3 autres en découlent facil^t.

1) $n = \# A$, $p = \# B$

$\varphi : [\![1,n]\!] \xrightarrow{\sim} A$, $\psi : [\![1,p]\!] \xrightarrow{\sim} B$

si $A\cap B = \emptyset$, construisons une bijection

de $[\![1, n+p]\!]$ ds $A\sqcup B$.

posons : $\chi : [\![1, n+p]\!] \longrightarrow A \sqcup B$

$$x \longmapsto \begin{cases} \varphi(x) & \text{si } x \leq n \\ \psi(x-n) & \text{si } x > n \end{cases}$$

Mq. χ est bien définie

- si $x \leq n$, $x \in [\![1, n]\!]$ donc $\varphi(x)$ existe
  donc $\chi(x)$ existe, et $\chi(x) \in A$, donc $\chi(x) \in A \sqcup B$
- si $x > n$, alors $x \in [\![n+1, n+p]\!]$
  donc $x - n \in [\![1, p]\!]$ donc $\psi(x-n)$ existe
  donc $\chi(x)$ existe et $\chi(x) \in B$
  donc $\chi(x) \in A \sqcup B$.

Mq. χ est injective : Soit $x, y \in [\![1, n+p]\!]$ tq.

$\chi(x) = \chi(y)$ • si $x \in [\![1,m]\!]$, $y \in [\![m+1,m+p]\!]$,

alors $\chi(x) \in A$ et $\chi(y) \in B$

or $A \cap B = \emptyset$ dc $\chi(x) \neq \chi(y)$: absurde.

dc : soit $x,y \in [\![1,m]\!]$, soit $x,y \in [\![m+1,m+p]\!]$.

• si $x,y \in [\![1,m]\!]$: $\chi(x) = \chi(y) \Rightarrow \varphi(x) = \varphi(y)$

$\Rightarrow x = y$ car φ est injec.

• si $x,y \in [\![m+1,m+p]\!]$, $\chi(x) = \chi(y) \Rightarrow \psi(x-m) = \psi(y-m)$

$\Rightarrow x-m = y-m$ car ψ injec

$\Rightarrow x = y$

Ds ts les cas, $x = y$, dc χ est injec.

Mq. χ est surjec : Soit $y \in A \sqcup B$.

- si $y \in A$: φ est surjective donc il existe $x \in [\![1, n]\!]$ tq. $\varphi(x) = y$

  donc : $\chi(x) = y$.

- si $y \in B$: ψ est surjec donc il existe $t \in [\![1, p]\!]$ tq. $\psi(t) = y$ donc en posant $x = t + n$, on a $x \in [\![n+1, n+p]\!]$ donc :

$$\chi(x) = \psi(x-n) = \psi(t) = y$$

dans tous les cas, y a 1 antécédent par χ, donc χ est surjec..

donc χ est bijec, donc $\# A \sqcup B = n + p = \# A + \# B$.

autre méthode : on pose $\mathcal{C} : A \cup B \longrightarrow [\![1, n+p]\!]$

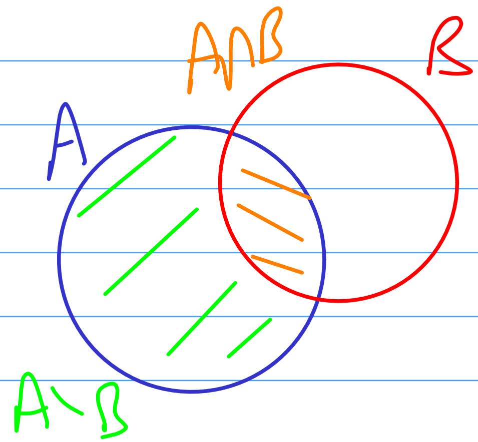
$$x \longmapsto \begin{cases} \varphi^{-1}(x) & \text{si } x \in A \\ \psi^{-1}(x) + n & \text{si } x \in B \end{cases}$$

Rq : • $\mathcal{C}$ est bien défini car si $x \in A \cup B$, $x \in A$ ou $x \in B$, mais pas les 2 !

• $\mathcal{C} \circ \chi = id_{[\![1, n+p]\!]}$ et $\chi \circ \mathcal{C} = id_{A \cup B}$.

2) $A = (A \setminus B) \sqcup (A \cap B)$

(exo facile)



donc avec 1) :

$\# A = \#(A \setminus B) + \#(A \cap B)$

donc $\#(A \setminus B) = \# A - \#(A \cap B)$

3) On a : $A \cup B = B \sqcup (A \setminus B)$

avec 1) et 2) :

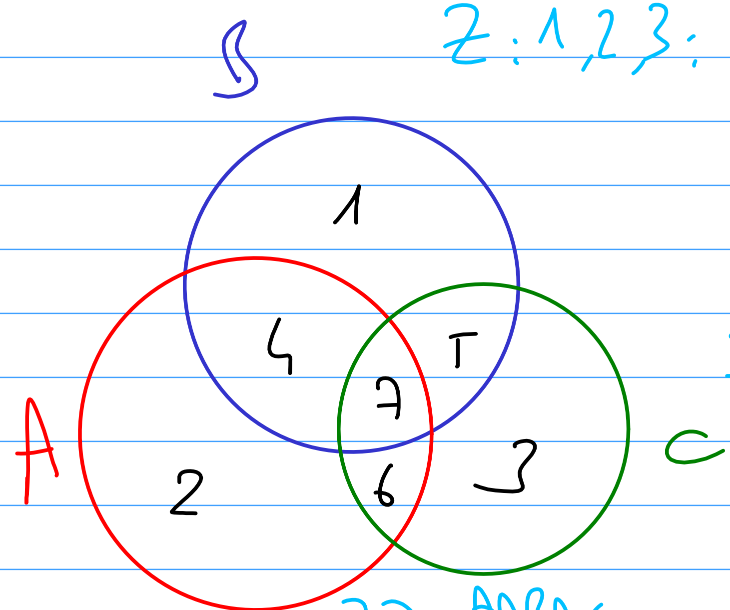
$$\# A \cup B \underset{1)}{=} \# B + \#(A \setminus B) \underset{2)}{=} \# B + \# A - \#(A \cap B)$$

4) $C_E A = E \setminus A$ avec 2) : $\# C_E A = \# E - \# A$.

Pb : $\# A \cup B \cup C$??

$\# A + \# B + \# C$:

les pts des zones 1, 2, 3 sont comptés 1 fois



Z : 1, 2, 3 : $\notin A \cap B$
$\notin A \cap C$
$\notin B \cap C$
$\notin A \cap B \cap C$

Z : 4, 5, 6 : sont ds $A \cap B$
ou $A \cap C$
ou $B \cap C$
mais pas $A \cap B \cap C$

Z 7 : $A \cap B \cap C$

Les pts des zones 4, 5, 6 ont comptés 2 fois
les pts de la zone 7 ont comptés 3 fois

$\#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) - \#(B \cap C)$:

zone 1, 2, 3 : 1 fois

zone 4, 5, 6 : 2 - 1 fois

zone 7 : 3 - 1 - 1 - 1 : 0 fois.

$\#(A \cup B \cup C) = \#A + \#B + \#C - \#A \cap B - \#B \cap C - \#A \cap C + \underbrace{\#A \cap B \cap C}_{= \text{zone } 7}$

Z 1, 2, 3 : 1 fois
Z 4, 5, 6 : 2 fois
Z 7 : 3 fois

Z 1, 2, 3 : 0 fois
Z 4, 5, 6 : -1
Z 7 : -3

Z 1, 2, 3 : 0 fois
Z 4, 5, 6 : 0 fois
Z 7 : +1 fois

Formule du crible de Poincaré : ex ? feuille 2.