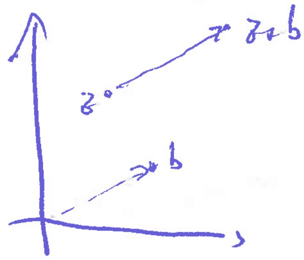
Tranformations du plan :

$\mathbb{R}^2 \simeq \mathbb{C}$, ~~z coordonnée~~ $z = x+iy$ coordonnées cartésiennes.

On veut étudier les applications $f(z) = az+b$ $\quad a \in \mathbb{C}^*, b \in \mathbb{C}$.

Cas 1 : $a=1$. $\quad f(z) = z+b$. est une translation



On note cette transformation τ_b $\quad \tau_b(z) = z+b$.

Calcul de $Fix(\tau_b)$:

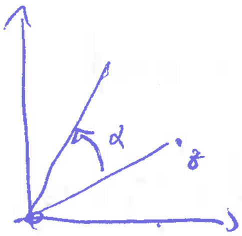
Il faut resoudre $\quad z = \tau_b(z) = z+b \iff b=0$.

Si $b \neq 0 \Rightarrow \nexists\, z$ tq. $z = \tau_b(z) \Rightarrow Fix(\tau_b) = \emptyset$

Si $b = 0 \Rightarrow \forall z \in \mathbb{C}$, $z = \tau_0(z) \Rightarrow \tau_0 = Id$ et $Fix(Id) = \mathbb{C}$.

Cas 2 : $|a| = 1$ mais $a \neq 1$. $\quad a = e^{i\alpha}$ $\quad \alpha \not\equiv 0 \pmod{2\pi}$

$z \mapsto e^{i\alpha} z$ est une rotation, qu'on note $\rho_{0,\alpha}$.
de centre 0.



effectivement, si $z = re^{i\theta}$

on a $e^{i\alpha} re^{i\theta} = r \cdot e^{i(\alpha+\theta)}$

Donc l'argument est augmenté de $\alpha \rightsquigarrow$ rotation de α.

En général, $f : z \mapsto e^{i\alpha} z + b$

$Fix(f) = ?$ $\quad$ si $z = f(z) = e^{i\alpha} z + b$ alors $z(1-e^{i\alpha}) = b \Rightarrow$

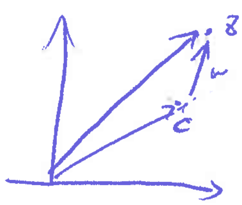
Car $\alpha \not\equiv 0 \pmod{2\pi} \Rightarrow e^{i\alpha} \neq 1$ et $z = \dfrac{b}{1-e^{i\alpha}} =: c$ est la seule solution $Fix(f) = \{c\}$.

On montre que f est la rotation d'angle α et centre c (notée $\rho_{c,\alpha}$)

~~Soit $z = c+w$ si $f(z)$~~

~~alors $f(w) = f(z-c) = e^{i\alpha}(z-c)+b = e^{i\alpha}z - \dfrac{e^{i\alpha}b}{1-e^{i\alpha}} + b$~~

~~$= e^{i\alpha} z + \dfrac{e^{i\alpha}}{\quad}$~~



CS - 0

Soit $\tau_c(z) = z + c$ la translation. $\quad c = \frac{b}{1-e^{i\alpha}}$

f est la rotation de centre c et angle $\alpha \Leftrightarrow f = \tau_c \circ \rho_{0,\alpha} \circ \tau_{-c}$.

$$\tau_c \circ \rho_{0,\alpha} \circ \tau_{-c}(z) = \tau_c \circ \rho_{0,\alpha}(z - c) = \tau_c(e^{i\alpha}(z-c)) = e^{i\alpha}(z-c) + c \overset{?}{=} e^{i\alpha}z + b$$

$$\Leftrightarrow -e^{i\alpha}c + c = b \Leftrightarrow c = \frac{b}{1-e^{i\alpha}}$$ ok

Cas 3 : $|a| = \cancel{]0,+\infty[}\ \mathbb{R}^+ \setminus \{1\} =]0,1[\cup]1,+\infty[$.

Si $f(z) = \lambda z$, f est l'homothétie de rapport λ ; $(h_{0,\lambda})$

en coordonnées exponentielles, $z = re^{i\theta}$, $\lambda z = \lambda r e^{i\theta}$

$\rightarrow$ l'argument ne change pas, et le module est multiplié par λ.

En général, f est l'homothétie de centre c et rapport λ $(h_{c,\lambda}) \Leftrightarrow$

$$f = \tau_c \circ h_{0,\lambda} \circ \tau_{-c} \qquad \tau_c(h_{0,\lambda}(\tau_{-c}(z))) = \tau_c(h_{0,\lambda}(z-c)) =$$

$$\tau_c(\lambda(z-c)) = \lambda(z-c) + c \quad = \lambda z + b \Leftrightarrow c = \frac{b}{\underset{\neq 1}{1-\lambda}}.$$

Encore une fois, $\mathrm{Fix}(h_{c,\lambda}) = \{c\}$.

En général, $f(z) = az + b$ est une <u>composition</u> de l'une de ces trois transformations. si $a = \lambda e^{i\alpha}$, alors $f = \tau_b \circ h_{0,\lambda} \circ \rho_{0,\alpha}$

° Taille des ensembles

Déf : Deux ensembles E, F sont <u>équipotents</u> (ont la même taille) si $\exists f : E \to F$ bijection. $(E \simeq F)$.

(Rmq. - si E est équipotent à F, alors F est équipotent à E :

$E \simeq F \Leftrightarrow F \simeq E$ $\quad f : E \to F$ bijectio $\Rightarrow f^{-1} : F \to E$ bijection réciproque.

- $E \simeq F$, $F \simeq G \Rightarrow E \simeq G$. : $f : E \to F$, $g : F \to G \Rightarrow g \circ f : E \to G$ est

bijections

une bijection (prop. 7, autre cours)

$E \simeq E$ $(\mathrm{id}_E : E \to E)$.

Ensembles finis.

Définition : Un ensemble E est <u>fini</u> s'il est vide ou s'il existe $n \in \mathbb{N}$ tel que $E \simeq \{1, \dots, n\}$

(E fini $\Leftrightarrow \exists\, n \in \mathbb{N} \mid E \simeq \{m \in \mathbb{N} \mid m < n\}$.

Théorème : $\forall n, k \in \mathbb{N}^*$, si $\exists$ injection $i : \{1, \dots, n\} \to \{1, \dots, k\} \Rightarrow n \leq k$.

Preuve : On procède par <u>récurrence</u> comme suit : Soit $P(n)$ la propriété :

$P(n)$: si $k \in \mathbb{N}^*$ et $\exists\, i : \{1, \dots, n\} \hookrightarrow \{1, \dots, k\}$, alors $n \leq k$.

$P(1)$ est vraie : si $\{1\} \hookrightarrow \{1, \dots, k\} \Rightarrow 1 \leq k$ (ok).

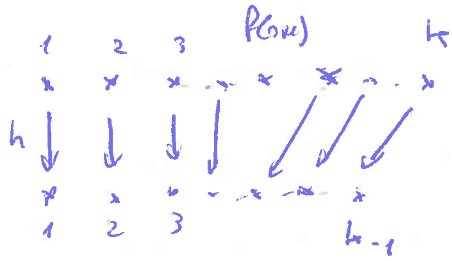
Supposons $P(n)$ vraie pour un certain $n \in \mathbb{N}^*$, et démontrons $P(n+1)$.

Soit $f : \{1, \dots, n+1\} \to \{1, \dots, k\}$ une injection pour $k \in \mathbb{N}^*$. On veut montrer $k \geq n+1$.

Comme $f(1) \neq f(n+1)$ par injectivité, on a $k \geq 2$.

Soit $h : \{1,\dots,k\} \setminus \{f(n+1)\} \longrightarrow \{1,\dots,k-1\}$ définie par :

$$h(i) = \begin{cases} i & \text{si } i < f(n+1) \\ i-1 & \text{si } i > f(n+1) \end{cases}$$



h est bijective.

$$h^{-1}(j) = \begin{cases} j & \text{si } j < f(n+1) \\ j+1 & \text{si } j \geq f(n+1) \end{cases}$$

L'application $h \circ f|_{\{1,\dots,n\}} : \{1,\dots,n\} \to \{1,\dots,k-1\}$ est injective

$\left(f(\{1,\dots,n\}) \subseteq \{1,\dots,k\} \setminus \{f(n+1)\} \text{ par injectivité de } f \right)$ La composée d'injections est injective.

Par $P(n)$ (hypothèse de récurrence), on a $n \leq k-1$, d'où $n+1 \leq k$ □

Corollaire: Si E est fini (et non vide), $\exists!\, n$ tel que $E \simeq \{1,\dots,n\}$.

Preuve: Supposons $E \simeq \{1,\dots,n\}$ et $E \simeq \{1,\dots,k\}$.

$\Rightarrow \exists$ bijection $f : \{1,\dots,n\} \to \{1,\dots,k\}$

Par le théorème, $n \leq k$.

" " appliqué à $f^{-1} : \{1,\dots,k\} \to \{1,\dots,n\}$, $k \leq n$.

$\Rightarrow n = k$. □

Définition: ~~Le Car~~ Soit E un ensemble fini.

On appelle le cardinal de E (ou la cardinalité de E), et on note $\#E$ ou $\mathrm{Card}(E)$, l'unique n tel que $E \simeq \{1,\dots,n\}$.

On pose $\mathrm{Card}(\emptyset) = 0$.

Propriétés du cardinal :

1) Si E est fini et $F \simeq E$ $\Rightarrow$ (F est fini et) $\#F = \#E$.

2) Soient E ensemble fini et $A \subseteq E$.

Alors A est fini et $\# A \leq \# E$. De plus, $A = E \iff \# A = \# E$

3) Soit $f: E \to F$ une application, et $A \subseteq E$ une partie finie de E.

Alors $f(A)$ est fini et $\# f(A) \leq \# A$. De plus, $\# f(A) = \# A \iff$

$f|_A$ est injective.

Preuve. 2) On procède par récursion sur $n = \# E$.

Si $n=1$, $A \subseteq E \Rightarrow A = E$ ou $A = \phi$. donc soit $\mathrm{Card}(A) = 0 < 1$

et $A \neq E$, soit $\mathrm{Card}(A) = 1$, $A = E$. ok.

Supposons que 2) est vérifié pour $\# E \leq n$, et montrons-le pour $\# E = n+1$

Soit $A \subseteq E$. Supposons $A = E$. alors ~~Card~~ A est fini, et $\mathrm{Card}(A) = \mathrm{Card}\, E$.

Supposons $A \subsetneq E$, et soit $x \in E \setminus A$. Donc $A \subseteq E \setminus \{x\}$.

Prop. E fini et $x \in E \Rightarrow \#(E \setminus \{x\}) = \# E - 1$. (et $E \setminus \{x\}$ est fini).

$\mathrm{Card}(E \setminus \{x\}) = n$. En effet, soit $f: E \to \{1, \ldots, n+1\}$ bijection, et

$h: \{1, \ldots, n+1\} \setminus \{f(x)\} \to \{1, \ldots, n\}$ donné par $h(i) = \begin{cases} i & i < f(x) \\ i-1 & i > f(x) \end{cases}$

h est bijective et donc $h \circ f|_{E \setminus \{x\}} : E \setminus \{x\} \to \{1, \ldots, n\}$ est une bijection, et

$\#(E \setminus \{x\}) = n$.

Par hypothèse récursive, A est fini et $\# A \leq \#(E \setminus \{x\}) = n < n+1$. $\square$

3) On procède par récurrence sur $\# A$.

Si $\# A = 0 \iff A = \phi \Rightarrow f(\phi) = \phi$ et l'énoncé est clair.

Soit $n \geq 0$. Supposons que l'énoncé soit vrai pour $\# A \leq n$. Supposons $\# A = n+1$

On choisit $x \in A$, et $B = A \setminus \{x\} \subsetneq A$

B est fini et $\# B = \underbrace{\# A - 1}_{n}$ (par la proposition)

Par hypothèse de récurrence $f(B)$ est fini et $\# f(B) \leq n$.

Mais $f(A) = f(B) \cup \{f(x)\}$

Si $f(x) \in f(B) \Rightarrow \# f(A) = \# f(B) \leq n$.

Si $f(x) \notin f(B) \Rightarrow \# f(A) \leq \# f(B) + 1 \leq n+1$

(Si $\# f(B) = k$, $g : f(B) \xrightarrow{\text{bij}} \{1, \dots, k\}$, on définit $g' : f(B) \cup \{f(x)\} \to \{1, \dots, k+1\}$,

$g'(y) = g(y)$ si $y \in f(B)$, $g'(f(x)) = k+1$. g' est bijective.)

Donc $\# f(A) \leq n+1 = \# A$ ok.

Supposons que $f|_A$ soit injective. Alors $f|_B$ est injective, et par hypothèse récursive, $\# f(B) = \# B$. Car $f|_A$ est injective, $f(x) \notin f(B)$ et

$\# f(A) = \# f(B) + 1 = \# B + 1 = \# A$. ok

Si $f|_A$ n'est pas injective, ~~on peut~~ $\exists x_1, x_2 \in A$ t.q. $f(x_1) = f(x_2)$.
Si on choisit $x = x_1$ on a $f(x_1) = f(\underset{B}{x_2}) \Rightarrow f(x) \in f(B)$

$\Rightarrow \# f(A) = \# f(B) \leq n$

$\square$

Théorème : Soient E, F deux ensembles finis tels que $\# E = \# F$, et $f : E \to F$ une application. Alors les trois propriétés suivantes sont équivalentes :
(a) f est injective (b) f est surjective (c) f est bijective.

Preuve : $(c) \Rightarrow (a)$, $(c) \Rightarrow (b)$. et $(a + b) \Rightarrow (c)$.

Il suffit de montrer que $(a) \Leftrightarrow (b)$

$\Rightarrow$ Par (3) de la proposition précédente, f injective $\Rightarrow \# f(E) = \# E = n$.

Donc $f(E) \subseteq F$ avec $\# E = \# F = n \overset{(2)}{\Rightarrow} f(E) = F$. ($f$ surjective).

$\Leftarrow$ Si f est surjective, $f(E) = F$. et $\# f(E) = \# F = \# E$.

f est donc injective par (3).

Proposition (Calcul des cardinaux)

1) Soit I un ensemble fini, et $(A_i)_{i\in I}$ une famille d'ensembles qui définit une partition de l'ensemble E.

On suppose que A_i est fini pour $\forall i \in I$. Alors E est fini et

$$\# E = \sum_{i\in I} \# A_i .$$

En particulier, $\#(A \sqcup B) = \#A + \#B$. (si A, B finis)

2) Si $A, B \subseteq E$ sont finis, alors $A \cup B$ est fini et

$$\#(A\cup B) = \#A + \#B - \#(A\cap B).$$

3) Soient E, F finis. Alors $E\times F$ est fini et $\#(E\times F) = \#E \cdot \#F$.

4) Soient E, F finis. L'ensemble $\mathcal{F}(E,F)$ est fini, et $\#\mathcal{F}(E,F) = (\#F)^{\#E}$

(D'où la notation $\mathcal{F}(E,F) = F^E$ ...)

Preuve : 1) Par récurrence sur $\# I$.

Si $\# I = 1$, il n'y a rien à montrer. Soit $n \geq 1$,

Supposons que l'énoncé soit vrai pour $\# I \leq n$.

Soit I t.q. $\# I = n+1$. Soit $j \in I$, $A = \bigcup_{i\in I\setminus\{j\}} A_i$, $B = A_j$.

alors $E = A \sqcup B$, avec A fini (par hypothèse récursive), B fini, et

$\# A = \sum_{i\neq j} \# A_i$. Notons $a = \# A$, $b = \# B$.

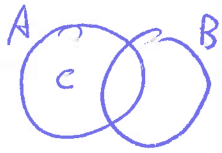
$\exists f : A \to \{1, \dots, a\}$, $g : B \to \{1 \dots b\}$ bijections.

On définit $h : E \to \{1, \dots a+b\}$. $h(x) = \begin{cases} f(x) & x \in A \\ a + g(x) & x\in B \end{cases}$.

h est une bijection, de bijection réciproque $h^{-1}(k) = \begin{cases} f^{-1}(k) & k \leq a \\ g^{-1}(k-a) & k > a \end{cases}$

Donc E est fini et $\# E = \# A + \# B = \sum_{i\in I} \# A_i$. $\square$

2) Posons $C = A \setminus B$. C est fini car $C \subseteq A$ fini (Prop(2))



Alors $A \cup B = C \sqcup B$, donc $\#(A\cup B) = \#C + \#B$ (par 1)

Mais $A = C \sqcup (A \cap B)$, donc $\#A = \#C + \#(A\cap B)$ (par 1).

D'où $\#(A\cup B) = \#C + \#B = \#A - \#A\cap B + \#B$.

3) Notons que la famille $(\{a\}\times F)_{a\in E}$ forme une partition de $E\times F$.

Notons que $\{a\}\times F \simeq F$ est fini. Par (1), $\#E\times F = \sum_{a\in E} \#F = \#E \cdot \#F$.

4) Notons $m = \#E$, $n = \#F$. [(Soit $f : E \to \{0,.., m\}$ et $g : F \to \{0,.., n\}$ deux bijections. Si $a : E \to F$ est une fonction, on peut lui associer
$\Phi(a) = \sum_{x\in E} g(x)\cdot n^{f(x)}$. Notons que $\Phi : \mathcal{F}(E,F) \to \{0,.., n^m - 1\}$ est une bijection)]

Construire une application $f : E \to F$ revient au procédé suivant.

Soient $\{x_1 \dots x_m\}_{\in E}$ les éléments de E. Il faut choisir $f(x_1) \in F$ ($\#F$ possibilités), $f(x_2) \in F$ ($\#F$ possibilités), ...

Donc $\#\mathcal{F}(E,F) = \prod_{x\in E} \#F = (\#F)^{\#E}$. □

Nombres de parties d'un ensemble fini

Théorème : Si E est un ensemble fini, alors $\#P(E)$ est fini et
$\#P(E) = 2^{\#E}$.

Preuve. L'application $\Phi : P(E) \to \mathcal{F}(E, \{0,1\})$ définie par

$$A \longmapsto \chi_A$$

$$\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

est une bijection. En effet :

$\Psi : \mathcal{F}(E, \{0,1\}) \to \mathcal{P}(E)$, $f \mapsto \{x \in E \mid f(x) = 1\}$ est sa bijection réciproque.

Donc $\# \mathcal{P}(E) = \# \mathcal{F}(E, \{0,1\}) = \# \{0,1\}^{\# E} = 2^{\# E}$. □

On peut maintenant calculer la cardinalité des ensembles de la forme

$P_n^k = \{ A \subseteq \{1, \dots, n\} \mid \# A = k \}$, pour tout $0 \leq k \leq n$, $k, n \in \mathbb{N}$.

Rmq : $P_n^0 = \{\emptyset\}$. $\Rightarrow \# P_n^0 = 1 \quad \forall n$.

$\mathcal{C} : \mathcal{P}(\{1,\dots,n\}) \to \mathcal{P}(\{1,\dots,n\})$ est une bijection $(\mathcal{C} \circ \mathcal{C} = \mathrm{Id})$

$A \longmapsto A^c$

Il ~~s'en suit que~~ ~~En~~ Si $\# A = k$ alors $\# A^c = n-k$

$(A \sqcup A^c = \{1, \dots, n\}$, on a vu que $\# A + \# A^c = \# \{1 \dots n\} = n$.

Il s'en suit que $\mathcal{C}(P_n^k) = P_n^{n-k}$ et $\# P_n^k = \# P_n^{n-k}$.

Théorème : Soient $k, n \in \mathbb{N}$ t.q. $0 \leq k \leq n$. Alors $\# P_n^k = C_n^k = \binom{n}{k}$.

Rappelle, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ binomiale. $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k} \quad \forall 1 \leq k \leq n$

Lemme : $\forall k, n \in \mathbb{N}$, $1 \leq k < n$, on a $\# P_n^k = \# P_{n-1}^k + \# P_{n-1}^{k-1}$.

Preuve (lemme)

Soient $E = \{A \in P_n^k \mid n \in A\}$, $F = P_n^k \setminus E = \{A \in P_n^k \mid n \notin A\}$

Alors $P_n^k = E \sqcup F$, $\# P_n^k = \# E + \# F$.

L'application $E \to P_{n-1}^{k-1}$, $A \mapsto A \setminus \{n\}$ est une bijection, de réciproque $P_{n-1}^{k-1} \to E$, $B \mapsto B \sqcup \{n\}$.

l' ~~...~~ l'application $F \to P_{n-1}^k$ est une bijection
$$A \mapsto A$$

donc $\# P_n^k = \# E + \# F = \# P_{n-1}^{k-1} + \# P_{n-1}^k$. $\square$

Preuve (Théorème). On procède par récurrence sur n.

Les cas $n=0$ et $n=1$ sont clairs (par la remarque)

Pour $k=0$, $k=n$, on a $\# P_n^0 = \# P_n^n = \binom{n}{0} = \binom{n}{n} = 1$. (OK)

Supposons maintenant que $\# P_m^k = \binom{m}{k}$ pour $0 \leq k \leq m$, $m \leq n$.

On veut montrer que $\# P_{n+1}^k = \binom{n+1}{k}$ pour $1 \leq k \leq n$ (pour $k=0$, $k=n+1$ on l'a déjà fait)

Par le lemme, $\# P_{n+1}^k = \# P_n^{k-1} + \# P_n^k$.

Par hypothèse récursive, $\overset{\shortparallel}{\binom{n}{k-1}} + \overset{\shortparallel}{\binom{n}{k}}$.

Par les propriétés du binomial $\overset{\shortparallel}{\binom{n+1}{k}}$ $\square$.

Exemple : Il y a $\binom{7}{3} = \frac{7 \cdot 6 \cdot 5}{6} = 35$ possibilités de choisir 3 jours dans la semaine.

Corollaire. $\forall n \in \mathbb{N}$, on a $2^n = \sum_{k=0}^{n} \binom{n}{k}$.

Preuve : 1) C'est la formule du binome $(z+w)^n$ pour $z = w = 1$.

2) $\mathcal{P}(\{1, \dots, n\}) = \bigsqcup_{k=0}^{n} P_n^k$.

Par les propriétés de Card, $2^n = \mathrm{Card}(\mathcal{P}(\{1, \dots, n\})) = \sum_{k=0}^{n} \# P_n^k = \sum_{k=0}^{n} \binom{n}{k}$ $\square$

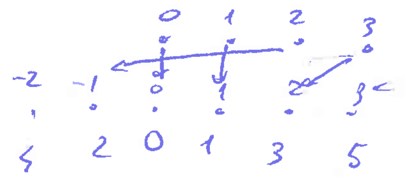
Ensembles dénombrables. (Partie pas trop précise...)

Définition. Un ensemble E est <u>dénombrable</u> si $E \simeq \mathbb{N}$ (équipotent).

Exemple 1) $2\mathbb{N}$ est dénombrable : $f : \mathbb{N} \to 2\mathbb{N}$, $n \mapsto 2n$ est une bijection.

2) $\mathbb{Z}$ est dénombrable.

L'application $f : \mathbb{N} \to \mathbb{Z}$ définie par

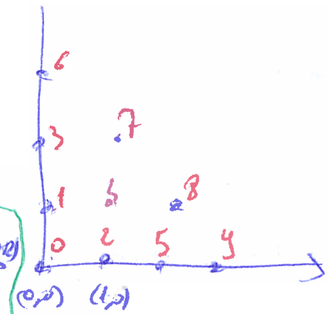


$$f(n) = \begin{cases} -m & \text{si } n = 2m,\ m \in \mathbb{N}. \\ m & \text{si } n = 2m-1,\ m \in \mathbb{N}^* \end{cases}$$

est une bijection, de réciproque

$$f^{-1}(m) = \begin{cases} -2m & \text{si } m \leq 0. \\ 2m-1 & \text{si } m > 0. \end{cases}$$

3) Le produit $\mathbb{N} \times \mathbb{N}$ est dénombrable :



$f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, $n \mapsto (f_1(n), f_2(n))$

$f_1(n) + f_2(n) = m$ si $\frac{m(m+1)}{2} \leq n < \frac{(m+1)(m+2)}{2}$

$f_1(n) = n - \frac{m(m+1)}{2}$. $\rightarrow$ $\left(n - \frac{m(m+1)}{2}, \frac{(m+1)(m+2)}{2} - n - 1\right)$ si $\frac{m(m+1)}{2} \leq n < \frac{(m+1)(m+2)}{2}$

réciproque $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.
$(p, q) \mapsto \frac{(p+q)(p+q+1)}{2} + p$

4) $\mathbb{Q}$ est dénombrable

5) $\mathbb{R}$ n'est pas dénombrable

Théorème : Soient E un ensemble dénombrable, et $A \subseteq E$.

Alors A est fini ou dénombrable.

Preuve. il suffit de montrer pour $E = \mathbb{N}$.

Si A est fini, il n'y a rien à montrer.

Supposons que A soit infini (C'est à dire, $\forall B \subset A$, B fini, on a $A \setminus B \neq \emptyset$)

On peut construire par récurrence une bijection $f : \mathbb{N} \to A$.

On pose ~~par~~ $f(0) = \min\{n \mid n \in A\}$. le plus petit élément de A.

(Attention ! le min existe ...)

Supposons qu'on a défini $f(0) < f(1) < \dots < f(n)$.

On définit $f(n+1) = \min\{m \in A_n\}$. $A_n = A \setminus \{f(0), \dots, f(n)\}$

$A_n \neq \emptyset$ car A est infini.

f est injective (car $f(0) < f(1) < \dots < f(n) < \dots$)

f est aussi surjective : supposons que $f(\mathbb{N}) \subsetneq A$. soit $B = A \setminus f(\mathbb{N})$ et $b = \min\{m \in B\}$. $f(\mathbb{N}) \cap \{m \leq b\}$ est contenu dans $\{0, \dots, b\}$, et donc il est fini. Il s'en suit que ~~$f^{-1}(B)$ est~~ $\{n \in \mathbb{N} \mid f(n) < b\}$ est fini, égal à $\{1 \dots k\}$ pour un certain k. Mais alors $f(k+1) = \min\{A \setminus \{f(\cancel{0}), \dots, k\}\} = b$. contradiction.

$\square$

Corollaire : $\mathbb{Q}$ est dénombrable (~~...~~ $\mathbb{Q} \subseteq \mathbb{Z} \times \mathbb{N}$ qui est dénombrable, et $\mathbb{Q}$ n'est pas fini)

Théorème (Cantor, 1892). Soit E un ensemble. Alors il n'existe pas de surjection $E \to P(E)$.

Preuve : Soit $f : E \to P(E)$ une application.

Soit $\Delta = \{ e \in E \mid e \notin \underbrace{f(e)}_{\subseteq E} \}$.

On veut montrer que $\Delta \notin f(E)$.

Supposons par absurde $\exists d \in E$ t.q. $f(d) = \Delta$.

alors $d \in \Delta \Leftrightarrow d \notin f(d) = \Delta \Leftrightarrow d \notin \Delta$: contradiction. $\square$

Corollaire : $P(\mathbb{N})$ est infini non-dénombrable.